

FortiGate Connector for Cisco ACI - Administration Guide

Version 1.3

FORTINET DOCUMENT LIBRARY

<http://docs.fortinet.com>

FORTINET VIDEO GUIDE

<http://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

<http://cookbook.fortinet.com/how-to-work-with-fortinet-support/>

FORTIGATE COOKBOOK

<http://cookbook.fortinet.com>

FORTINET TRAINING SERVICES

<http://www.fortinet.com/training>

FORTIGUARD CENTER

<http://www.fortiguard.com>

FORTICAST

<http://forticast.fortinet.com>

CLI REFERENCE

<http://cli.fortinet.com>

END USER LICENSE AGREEMENT

<http://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdocs@fortinet.com



Thursday, February 16, 2017

FortiConnector for Cisco ACI v. 1.3 - Administration Guide

01-540-371313-20160505

TABLE OF CONTENTS

Change Log	6
Overview	7
Licensing	7
Terms and concepts	8
FortiGate VDOMs	8
FortiOS RESTful API	8
North/South and East/West Traffic	8
Features	9
Supported Features	9
Baseline features from v. 1.0 to v. 1.1	9
Additional features added in v1.2	9
Additional features added in v1.3	10
Unsupported Features	10
Supported Fortinet Products	11
Models	11
Unknown models	11
Firmware Versions	11
Prerequisites	12
Cisco Side	12
FortiGate Side	12
Physical Firewall	12
VM Firewall	12
Components of the Device Package	14
Device model or specification	14
Device script	14
Directory of supporting files	14
Image file or directory	14
Operational modes	16
Go Through Mode (Layer 2)	16
Go To Mode (Layer 3)	16
Multi-tenant multi-device support	16
New Feature Deployment Guide	17
IPv6	17

IPv6 Interface Configuration.....	17
IPv6 Policy.....	17
IPv6 Dos.....	18
IPv6 Virtual IPs.....	19
Firewall Port Forwarding (Destination NAT).....	19
IP Pool Configuration.....	19
IPv4 Virtual IPs.....	20
DNAT Enable on Policy.....	21
Device Health.....	22
Interface Statistic.....	22
Dynamic EPG Notification.....	23
Supported use scenarios.....	26
Physical Fortigate.....	26
Go-Through Mode for west-east traffic within data center in ACI.....	26
Go-To Mode for north-south traffic for Web Server to access DataBase server in data center.....	26
Virtual Fortigate.....	26
Go-Through Mode for west-east traffic within data center in ACI.....	26
Go-To Mode for north-south traffic for Web Server to access DataBase server in data center.....	26
Deployment Procedures.....	27
Device package installation.....	27
Service Deployment.....	27
Importing the Device Package.....	28
Remove Device Package.....	28
Basic Steps to add Fortinet Firewall L4-L7 Virtual Device.....	29
Add L4-L7 Device.....	29
GENERAL.....	30
CONNECTIVITY.....	30
CREDENTIALS.....	30
Device 1.....	30
Cluster.....	31
Create Functional Profile Group.....	31
Create a Function Profile.....	32
Review.....	33
Service Graph.....	34
Create Service Graph.....	34
Deploy Service Graph.....	35
Modify Service Graph.....	35
Remove Service Graph.....	36
Service Graph deployed.....	38
Installation Variations.....	39

Deploying Data Center Layer 2 Segmentation with Cisco ACI and FortiGate.....	39
Pre-requisites.....	39
Work Flow.....	39
Configuration.....	40
Deploying Data Center Layer 3 Segmentation with Cisco ACI and FortiGate.....	45
Introduction.....	45
Prerequisites.....	45
Work Flow.....	46
Configuration.....	47
Deploying Firewall Service for North-to-South traffic with OSPF.....	61
Introduction.....	61
Prerequisites.....	61
Work Flow.....	62
Configuration.....	62
Deploying High Availability Service with Cisco ACI and FortiGate.....	77
Pre-requisite.....	77
Work Flow.....	77
Deploying Firewall service with Fortigate-VM and VMware.....	79
Pre-requisite.....	79
Work Flow.....	79
Configuration.....	79
Deploy the firewall device shared by multiple service graphs.....	84
Pre-requisite.....	84
Work Flow:.....	84
Configuration.....	85
Deploy the firewall device with shared interfaces through multiple service graphs.....	96
Pre-requisite.....	96
Basic Topology.....	96
Work Flow:.....	96
Configuration.....	97
Deploy the firewall device in a one-arm configuration with policy based redirect.....	109
Prerequisites.....	109
Basic Topology.....	110
Work Flow:.....	110
Configuration.....	111
APIC Infrastructure and FortiGate rollback.....	125
Basic Troubleshooting.....	126
Verify Service Graph deployed.....	126
Service deployed but parameters missing.....	127

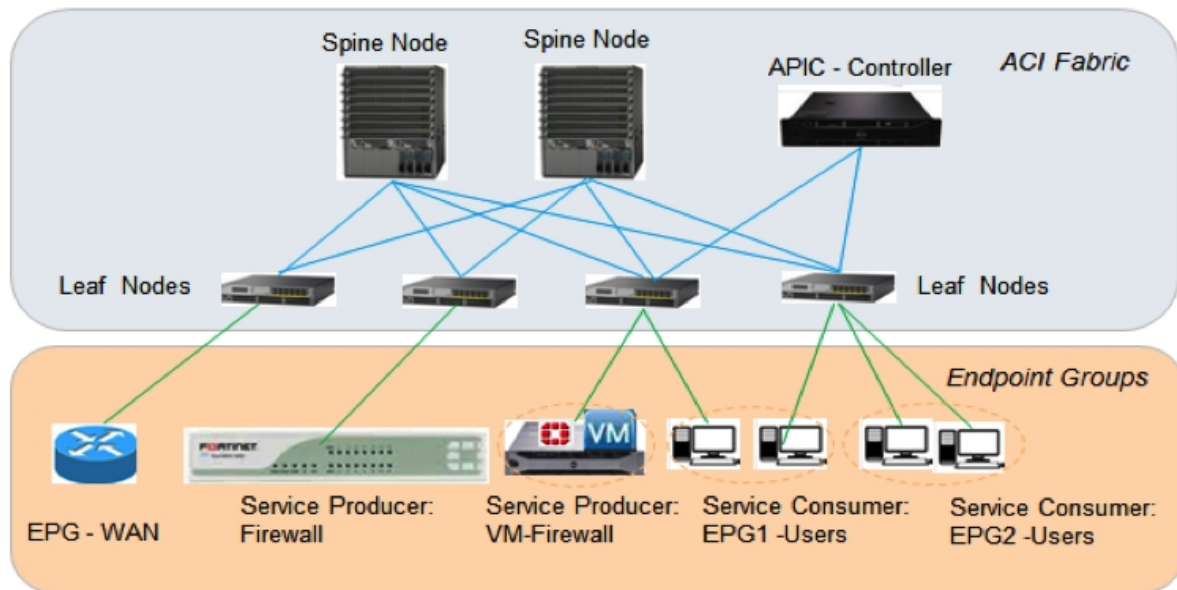
Change Log

Date	Change Description
2016-08-26	Initial Release of version 1.3

Overview

FortiGate Connector for Cisco ACI (Application Centric Infrastructure) is the Fortinet solution to provide seamless integration between Fortinet Firewall (Fortigate) deployments and the Cisco APIC (Application Policy Infrastructure Controller). This integration allows customers to perform single point of FortiGate configuration and Management operation through Cisco APIC.

While the FortiGate series of firewalls enable superb firewall services, in a data center environment, the insertion, configuration, and management of network services such as firewall can be quite complex and potentially error-prone tasks. One solution for such data center problems is Cisco's ACI. Cisco's ACI is a policy-based framework with integration of software and hardware in the underlying leaf-spine fabric. In Cisco ACI, the APIC is a tool used to automate service insertion and provisioning into the fabric of the network environment. Network service appliances, both physical and virtual, can be attached to ACI fabric's leaf node through APIC. Traffic demanding certain network services is steered by APIC-managed policies to the appropriate resources. The FortiGate Connector allows FortiGates to be included amongst the list of resources that traffic can be directed to.



Licensing

FortiGate Connector for Cisco ACI is free of charge for Fortinet customers. You need to make sure that you register your FortiGate with FortiCare on support.fortinet.com.

Terms and concepts

FortiGate VDOMs

VDOM or Virtual Domain refers to a discretely administered segment on a FortiGate firewall. A FortiGate firewall that is not segmented and where a single administrator can access all of the firewall is operating in the “root” VDOM. However, it is possible to segment the FortiGate so that different administrators can access different areas of the FortiGate. Credentials for VDOM X will allow access to the resources and settings of VDOM A but no other. There will also be global resources and settings that will require credentials to the root VDOM. When setting up connectivity between Cisco APIC and the FortiGates it will be important to know which VDOMs control the needed resources.

FortiOS RESTful API

REST (sometimes spelled ReST) stands for Representational State Transfer. It is a software architectural style for the WWW. REST systems typically communication over HTTP, using HTTP verbs or commands to retrieve and send information to remote servers.

A good resource for the finer details of Fortinet's implementation of ReST can be found at http://docs.fortinet.com/uploaded/files/1276/FortiAuthenticator_REST_API_Solution_Guide.pdf

North/South and East/West Traffic

The cardinal compass direction terms to describe traffic flow are used to differentiate between traffic within the cloud or data center and traffic going in and out of the cloud or data center.

- North/South - traffic either heading into or out of a cloud or data center.
- East/West - traffic that is between nodes inside the same cloud or data center.

Features

There are a number of features associated with firewalls in general and FortiGate firewalls in particular. This section should explain which of these features are available through the FortiGate Connector and which are not.

Supported Features

The FortiGate Connector for Cisco ACI supports the following functions:

Baseline features from v.1.0 to v.1.1

- Cisco ACI service insertion - software package for FortiGate device deployed to Cisco APIC, containing FortiGate models, function description, version, credentials, as a L4-L7 service.
- Enable tenant configuration to add/modify/delete L4-L7 device of FortiGate firewall service.
- Enable FortiGate deployment as both physical and virtual device (FortiGate chassis & VM).
- Support both transparent (GoThrough) and L3 (GoTo) device mode .
- Automatically create VDOM (context). One VDOM per logical device under a tenant.
- Enable FortiGate specific interface configuration: physical interface and port channel.
- Support IP address configuration on Layer 3 interfaces.
- Support subnet and service object configuration.
- Enable FortiGate firewall device to connect to endpoint groups (EPGs).
- Support IPv4 policies: match, action, network operations & security features' selection.
- Support NAT.
- Enable service graph to add/modify/delete FortiGate firewall service node
- Multiple interfaces can be added in the same device
- Single logical port can be shared in the same EPG for multiple service graphs
- Single VDOM can be used in multiple service graphs

Additional features added in v1.2

- High Availability (Active-Standby Mode)
- OSPF based routing configuration in the L3 (GoTo) mode
- Support for logging and error reporting of Fortigate as a L4-L7 device
- Automatically create VDOM based on APIC virtual device ID
- Policy enable/disable support
- Enable/Disable DDoS features
- Enable/Disable UTM Security Profiles

Additional features added in v1.3

- IPv6 Policy Configuration
- Firewall Port Forwarding (Destination NAT)
- APIC Dynamic EPG Notification
- Monitor Fortigate Devices (Health) Status
- Fortigate Device Packet Statistics on physical port

Unsupported Features

The following features normally found on FortiGates are not supported through the FortiGate Connector for Cisco ACI.

- Proxy Policy
- SSL/SSH Inspection
- FortiGate WAN load balance link.
- Administrator profile for limited access of different administrator accounts.
- Firewall port forwarding (destination NAT).
- Firewall logging: allowed traffic, security events, all sessions, etc.
- Firewall packet capture.
- Firewall with FortiGuard DDNS.
- Other Firewall features not specifically listed as supported.

The unsupported features on APIC may still be used on FortiGate outside of the APIC control; the user must login to FortiGate to configure, monitor, and debug. However, any conflict with the operations from APIC may cause malfunction.

Supported Fortinet Products

The supported Fortinet products refers to those that are compatible with the FortiGate Connector for Cisco ACI software, and will properly integrate into the Cisco ACI. The products are separated into models and firmware but it is an “and” set of parameters. In order to be supported the Fortinet product has to be one of the listed models running supported firmware.

Models

FortiGate Connector for Cisco ACI v1.3 supports the following predefined models:

- FG-300D
- FG-600D
- FG-900D
- FG-1000C
- FG-1000D
- FG-1200D
- FG-1500D
- FG-3000D
- FG-3100D
- FG-3200D
- FG-3700D
- FG-VM

Unknown models

The use of FortiGate Connector can be attempted with any FortiGate model, but do so with caution. Only those listed above have been confirmed. If an unknown model of FortiGate is used, the user needs to verify port names match the real FortiGate model.

Firmware Versions

FortiGate Connector v1.3 for Cisco ACI is compatible with the following FortiOS firmware:

- FortiOS 5.4 and above

Prerequisites

Cisco Side

Before the FortiGate Connector for Cisco ACI can be successfully deployed, a number of prerequisites need to be satisfied within the Cisco environment.

One of the following Cisco ACI environments needs to be in place:

- Cisco ACI v1.2(2h) or later

Within the Cisco ACI, the following configurations need to be completed before Layer 4 -7 Services (in this case, the FortiGate Connector) can be deployed:

- Creation of Access Policies configuration under Fabric menu
- Creation of any need Tenant(s)
- Creation of Network(s) (including Bridge Domain)
- Creation of Application Profile(s)
- Creation of End Point Group(s)
- Creation of Contract(s)
- Create OSPF L3Out (Only if OSPF is required)

For detail, please consult Cisco APIC deployment Guide.

http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/L4-L7_Services_Deployment/guide/b_L4L7_Deploy.html

FortiGate Side

Before the FortiGate Connector for Cisco ACI can be successfully deployed, a number of prerequisites need to be satisfied on the FortiGate side of the equation.

Physical Firewall

1. Configure administrator user name and password.
2. Enable http/https on mgmt. port.
3. Configure IP address in mgmt. port.
4. Enable VDOM-Admin globally.
5. Configure Port-Group if needed.

VM Firewall

1. Assign network ports before start VM
2. Configure administrator user name and password.
3. Enable http/https on mgmt. port.

4. Configure IP address in mgmt. Ports
5. Enable VDOM-Admin globally

Components of the Device Package

To add a network service to ACI fabric, the service's device package needs to be uploaded to APIC. The device package is a zip file containing these components:

Device model or specification

The Device Specification is an XML file called `DeviceModel.xml` that covers descriptions of FortiGate devices, interfaces, connectivity and services. The file contains a hierarchical description of FortiGate devices, including:

- Device functions
- Parameters of each function
- Interfaces/network connectivity information of each function.

Device script

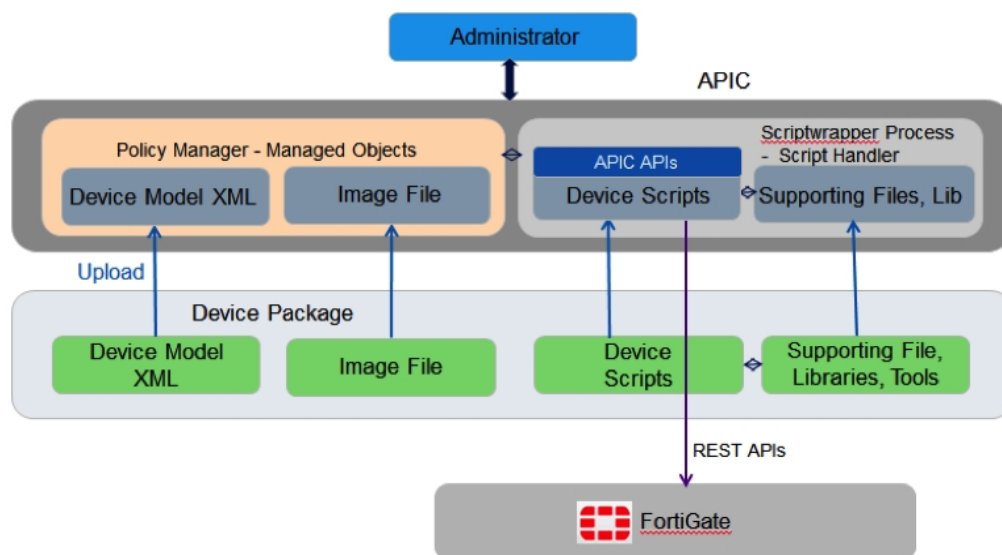
This is a Python file, `DeviceScript.py` with API functions to interface between the Cisco APIC and the FortiGate REST APIs. This Python file is associated by the `DeviceModel.xml` device specification to device script for APIC.

Directory of supporting files

This component contains supporting Python files, text files and libraries of scripts and tools.

Image file or directory

The directory contains file(s) such as a Fortinet icon (`Fortinet_name.gif`) to be displayed on the APIC management page. There are two types of network service devices which Cisco APIC integrates with. These types of devices are defined by their operation mode. They are either Go Through or Go To. Normally a device as to be preconfigured as one of these types before its imported package is managed by the APIC.



Operational modes

There are two types of network service devices which Cisco APIC integrates with. These types of devices are defined by their operation mode. They are either Go Through or Go To. Normally a device has to be preconfigured as one of these types before its imported package is managed by the APIC.

Go Through Mode (Layer 2)

Devices in Go Through mode are considered layer 2 devices (from the OSI model) and are sometimes known as transparent. They are referred to as transparent because while the traffic goes through them and can be affected by them, they are not seen by the network and are not a destination in their own right for the traffic. They do not route traffic. These devices are not referred to by the packet's destination MAC or IP address. In most cases, these devices will only have an address for the purposes of management.

Go To Mode (Layer 3)

Devices in Go To mode are considered Layer 3 (from the OSI model) devices. They can route traffic and they are referenced as the destination in a packet's destination MAC address or destination IP address.

Multi-tenant multi-device support

- Multi-tenant Multi-device is typical in the use cases of this project. The support is worth more detailed description. When FortiGate device is added a tenant's L4-L7 services, multi-context aware can be enabled. This indicates to the device package that the L4-L7 device is going to be a virtual device that shares resources with other tenants on the FortiGate. In FortiGate implementation, this virtual device is represented by a VDOM. Under each tenant, multiple such virtual devices can be configured. VDOM name is the virtual device ID generated by APIC when a virtual device is added.
- Each tenant sees all available interfaces and can share interfaces (ports) with other tenants, if it is multi-context aware. For Physical Device under L3 Routed (GoTo) Mode, Tenant can share physical interface as VLAN is used to isolate the physical interface. In VM Device, this is not true. You can only use dedicated VNIC.

New Feature Deployment Guide

IPv6

IPv6 Interface Configuration

We now support IPv6 configuration on interface level. Please consult below screen shot.

L4-L7 Services Function Profile - 3719

General Faults History

Properties

Name: 3719
Description:
Associated Function: Fortinet-FGAPC-1.3/Firewall

FEATURES AND PARAMETERS

Basic Parameters All Parameters

Meta Folder/Param Key Name Value Mandatory Locked Shared

Device Config	Device				
DeviceInterface	external		false	false	false
AllowAccess	AllowAccess-Default			false	false
Device IP Address(ex. 10.160.11.1 or 0.0.0.0(transparent))	IPAddress	16.1.1.1	false	false	false
Device IP Netmask(ex. 255.255.255.0)	IPNetmask	255.255.255.0	false	false	false
Device IPv6 Address(ex. ...)	IPv6IPAddress	FE80:0000:0000:0000:0202:B3FF:FE1E:8329	true	false	false
Device IPv6 Netmask(ex. 0)	IPv6IPNetmask	64	false	false	false
Interface IPv6 Address Mode(static, dhcp, pppoe)	IPv6Mode	static	true	false	false
Interface Address Mode(static, dhcp, pppoe)	mode	static	true	false	false
DeviceInterface	internal		false	false	false
Function Config	Function				
Network	Network		false	false	false
Policy and Objects	PolicyObjects		false	false	false
VDOM-Folder	vdcm-folder		false	false	false

IPv6 Policy

Once we configured IPv6 addresses onto interfaces, we can configure IPv6 policy to enforce the traffic. Please consult below screenshot.

L4-L7 Services Function Profile - 3719

General Faults History

Properties

Name: 3719

Description:

Associated Function: Fortinet-FGAPIC-1.3/Firewall

FEATURES AND PARAMETERS

Basic Parameters All Parameters

Meta Folder/Param Key Name Value Mandatory Locked Shared

IPV4 IP Pool	IPV4FWPPoolFolder		false	
IPV4 Policy	IPV4FWPolicyFolder		false	
IPV4 VIP	IPV4FWVIPFolder		false	
IPV6 DoS Policy	IPV6DoS-PolicyFolder		false	
IPV6 FirewallAddresses	IPV6FWAddressFolder		false	
IPV6 Policy	IPV6FWPolicyFolder		false	
FirewallPolicyRuleID(Number Only - EX. 1,2,...)	100		false	
Action(accept/deny/dst-vpn)	accept	false	false	
Destination Address or VIP	DestAddr/VIP		false	
Incoming interface(internal/external)	InInterface	internal	false	false
Name	Name	IPV6_policy	false	false
OrderNo	OrderNo	100	true	false
Outcoming interface(internal/external)	OutInterface	external	false	false
Source Address Folder	SrcAddrFolder		false	false
schedule list name	schedule-list-name	PolicyObjects/ScheduleFolder/always	false	false
Service	service-list-name	PolicyObjects/FWServiceFolder/ALL	false	false
Enable This Policy	status	enable	false	false
IPV6 VIP	IPV6FWVIPFolder		false	
ScheduleFolder	ScheduleFolder		false	
VDOM-Folder	vdom-folder		false	false

IPv6 Dos

Optionally, we can configure IPv6 Dos feature. Please consult below screenshot.

L4-L7 Services Function Profile - 3719

General Faults History

Properties

Name: 3719

Description:

Associated Function: Fortinet-FGAPIC-1.3/Firewall

FEATURES AND PARAMETERS

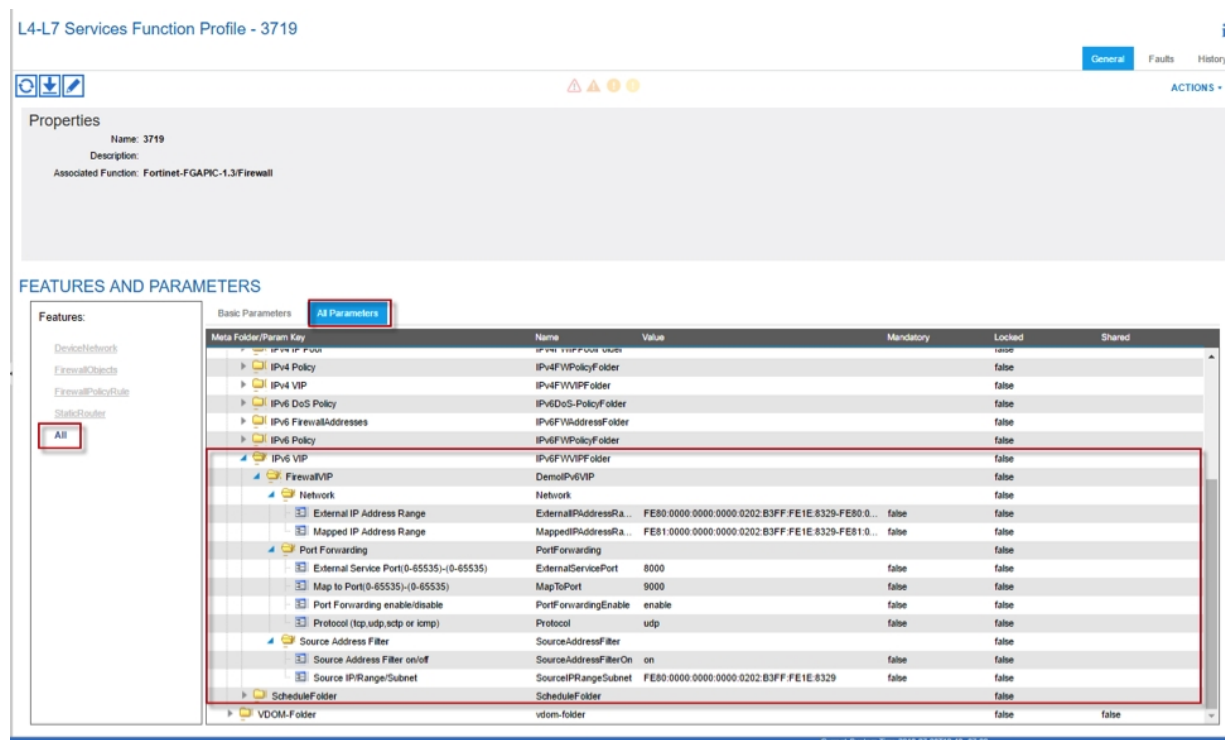
Basic Parameters All Parameters

Meta Folder/Param Key Name Value Mandatory Locked Shared

IPV4 Policy	IPV4FWPolicyFolder		false	
IPV4 VIP	IPV4FWVIPFolder		false	
IPV6 DoS Policy	IPV6DoS-PolicyFolder		false	
IPV6 DoS Policy	IPV6DoS		false	
OrderNo	OrderNo	10	true	false
DoS policy id	dos_policyid		false	false
Destination Address	dstaddr	PolicyObjects/IPV6FWAddressFolder/all	false	false
icmp_dst_session	icmp_dst_session		false	false
icmp_flood	icmp_flood		false	false
icmp_src_session	icmp_src_session		false	false
icmp_sweep	icmp_sweep		false	false
Incoming interface(internal/external)	interface	internal	false	false
ip_dst_session	ip_dst_session		false	false
ip_src_session	ip_src_session		false	false
sctp_dst_session	sctp_dst_session		false	false
sctp_flood	sctp_flood		false	false
sctp_scan	sctp_scan		false	false
sctp_src_session	sctp_src_session		false	false
Service	service	PolicyObjects/FWServiceFolder/ALL	false	false
Source Address	srcaddr	PolicyObjects/IPV6FWAddressFolder/all	false	false
Enable This Policy	status	enable	false	false
tcp_dst_session	tcp_dst_session		false	false

IPv6 Virtual IPs

In addition, we can configure IPv6 Virtual IP feature which you can apply to IPv6 Policy. Please consult below screenshot.



Firewall Port Forwarding (Destination NAT)

IP Pool Configuration

Below screenshot illustrated how to define IPv4 IP Pool. Due to the layout format ACI is providing, we have to list all the sub-features within the IP Pool. Please consult Fortigate Configuration Guide for option(s) that goes with appropriate Sub-feature. Otherwise, we will see error when push configuration from APIC down to Fortigate. From a very high level, here is the break down lay out of the Sub-feature and the accommodated options.

Dynamic IP Pool				
IP Pool type	IPv4 Pool			
Name				
Comments				
Type	Overload	One-to-One	Fixed Port Range	Port Block Allocation
External IP Range	X	X	X	X

Dynamic IP Pool				
Internal IP Range	N/A	N/A		N/A
Block Size	N/A	N/A	N/A	x
Blocks per User	N/A	N/A	N/A	x
ARP Reply	x	x	x	x

L4-L7 Services Function Profile - 3719

General Faults History

Properties

Name: 3719

Description:

Associated Function: Fortinet-FGAPIC-1.3/Firewall

FEATURES AND PARAMETERS

Basic Parameters All Parameters

Meta Folder/Param Key Name Value Mandatory Locked Shared

IP v4 & v6 Firewall Rules	IP v4 & v6 Firewall Rules				
IP v4 IP Pool	IP v4 IP Pool				
IP v4 Policy	IP v4 Policy				
IP v4 VIP	IP v4 VIP				
IP v6 DoS Policy	IP v6 DoS Policy				
IP v6 FirewallAddresses	IP v6 FirewallAddresses				
IP v6 Policy	IP v6 Policy				
FirewallPolicyRuleID(Number Only - EX. 1,2,...)	100				
Action(accept/deny/ssl-vpn)	accept	false	false		
Destination Address or VIP	DestAddr/VIP		false		
Incoming interface(internal/external)	InInterface	internal	false	false	
Name	Name	IPv6_policy	false	false	
OrderNo	OrderNo	100	true	false	
Outcoming interface(internal/external)	OutInterface	external	false	false	
Source Address Folder	SrcAddr Folder		false	false	
schedule list name	schedule-list-name	PolicyObjects/ScheduleFolder/always	false	false	
Service	service-list-name	PolicyObjects/FWServiceFolder/ALL	false	false	
Enable This Policy	status	enable	false	false	
IP v6 VIP	IP v6 VIP				
Schedule Folder	Schedule Folder				
VDOM-Folder	vdom-folder				

Fortinet FortiGate v7.0.10 (2019.03.01) 19.03.2019

IPv4 Virtual IPs

IPv4 Virtual IP Pool can also configure for DNAT feature. Please consult below screenshot.

L4-L7 Services Function Profile - 3719

Properties

Name: 3719
Description:
Associated Function: Fortinet-FGAPIC-1.3/Firewall

FEATURES AND PARAMETERS

Basic Parameters **All Parameters**

Meta Folder/Param Key	Name	Value	Mandatory	Locked	Shared
IPv4 DoS Policy	IPv4DoSFolder			false	
IPv4 FirewallAddresses Group	IPv4FWAddrGrpFolder			false	
IPv4 FirewallAddresses	IPv4FWAddressFolder			false	
IPv4 IP Pool	IPv4FWIPPoolFolder			false	
IPv4 Policy	IPv4FWPolicyFolder			false	
IPv4 VIP	IPv4FWVIPFolder			false	
Firewall/VIP	DemolPv4VIP			false	
Network	Network			false	
External IP Address Range	ExternalIPAddressRa...	1.1.1.1-1.1.1.2	false	false	
Interface(internal/external/any)	Interface	any	false	false	
Mapped IP Address Range	MappedIPAddressRa...	2.2.2.1-2.2.2.2	false	false	
Port Forwarding	PortForwarding			false	
External Service Port(0-65535)-(0-65535)	ExternalServicePort	6000	false	false	
Map to Port(0-65535)-(0-65535)	MapToPort	7000	false	false	
Port Forwarding enable/disable	PortForwardingEnable	enable	false	false	
Protocol (tcp, udp, tcp or icmp)	Protocol	udp	false	false	
Source Address Filter	SourceAddressFilter			false	
Source Address Filter on/off	SourceAddressFilterOn	on	false	false	
Source IP Range/Subnet	SourceIPRangeSubnet	16.1.1.1/24	false	false	
IPv6 DoS Policy	IPv6DoS-PolicyFolder			false	
IPv6 FirewallAddresses	IPv6FWAddressFolder			false	

Current System Time 2018-07-08 10:10:47:05

DNAT Enable on Policy

Once above DNAT sub-components are configured, we can apply them to the Policy level. Please consult below screenshot for reference.

L4-L7 Services Function Profile - 3719

Properties

Name: 3719
Description:
Associated Function: Fortinet-FGAPIC-1.3/Firewall

FEATURES AND PARAMETERS

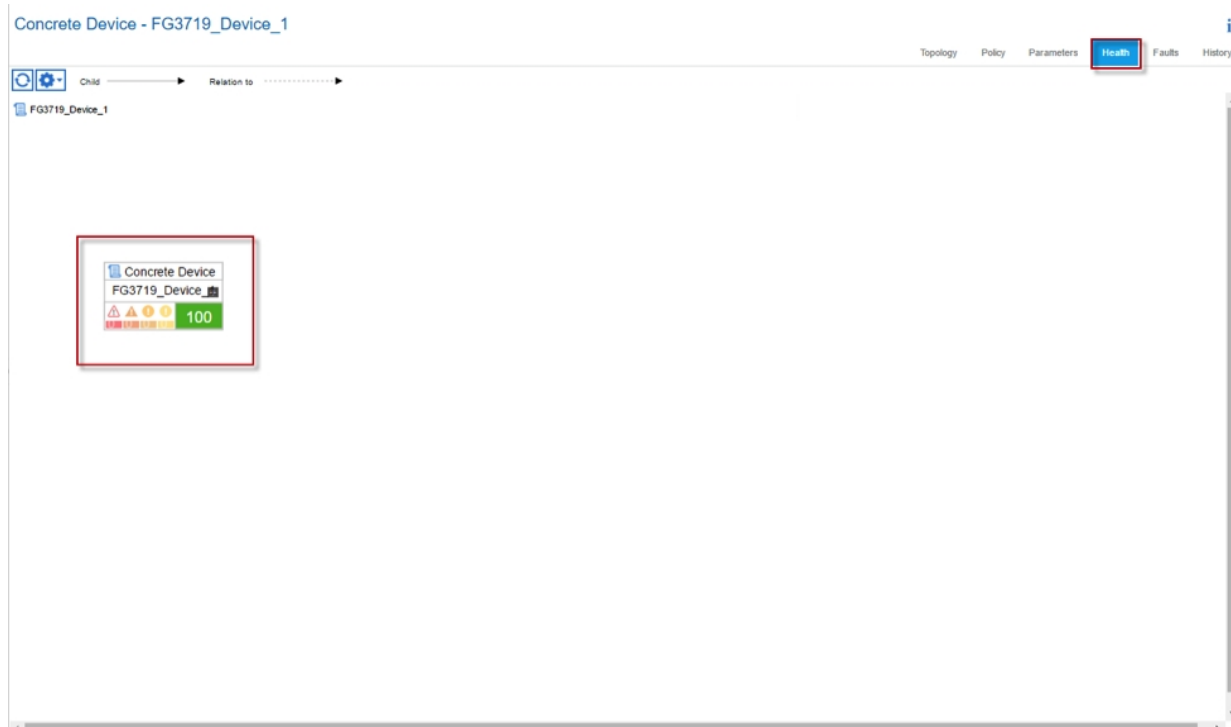
Basic Parameters **All Parameters**

Meta Folder/Param Key	Name	Value	Mandatory	Locked	Shared
IPv4 IP Pool	IPv4FWIPPoolFolder			false	
IPv4 Policy	IPv4FWPolicyFolder			false	
FirewallPolicyRuleID(Number Only - EX. 1.2.)	10			false	
Action(accept/deny/ssl-vpn)	Action	accept	false	false	
Destination Address or VIP	DestAddr/VIP			false	
Incoming interface(internal/external)	InInterface	internal	false	false	
LoggingOptions	Logging			false	
Name	Name	10	false	false	
NATFolder	NATFolder			false	
Fixed Port(enable/disable)	FixedPort	enable	false	false	
IP Pool Configuration	IPPoolConfigFolder			false	
IP Pool Config	IPPoolConfig	PolicyObjects/IPv4FWIPPoolFolder/DemolPv4IPPool	false	false	
IP Pool Configuration(enable/disable)	IPPoolConfigEnable	enable	false	false	
NAT(enable/disable)	NAT	enable	false	false	
OrderNo	OrderNo	10	true	false	
Outgoing interface(internal/external)	OutInterface	external	false	false	
SecurityProfiles	SecurityProfiles			false	
Source Address Folder	SrcAddrFolder			false	
schedule list name	schedule	PolicyObjects/ScheduleFolder/always	false	false	
Service	Service	PolicyObjects/FWServiceFolder/ALL	false	false	

Current System Time 2018-07-08 10:04:47:00

Device Health

From L4-L7 Device level, we can obtain the Fortigate Device Health. Navigate to **L4-L7 Services> L4-L7 Devices>Device Name> Concrete Device> Health Tab**, you can obtain the device health. Please consult below screenshot for reference.



Interface Statistic

From L4-L7 Device level, we can also obtain the Fortigate Interface Statistic. Navigate to **L4-L7 Services> L4-L7 Devices>Device Name> Concrete Device> Interface>Stats Tab**, you can observe interface statistic by enabling various statistic indicator such as RX/TX...etc. Please consult below screenshot for reference.



Dynamic EPG Notification

This feature allowing us to dynamically update of object group membership, where it corresponds to an End Point Group (EPG). You can dynamically add IP addresses/subnets based on endpoint/network attachment notification by ACI.

For this feature, we have created two groups “dyn_epg_ext_grp” and “dyn_epg_int_grp” which you can apply to the policy source field. When an end point is detected, notification will received from ACI and the endpoint IP will added to this membership group where policy will be applied.

L4-L7 Services Function Profile - 3719v2

General Faults History

Properties

Name: 3719v2

Description:

Associated Function: Fortinet-FGAPIC-1.3/Firewall

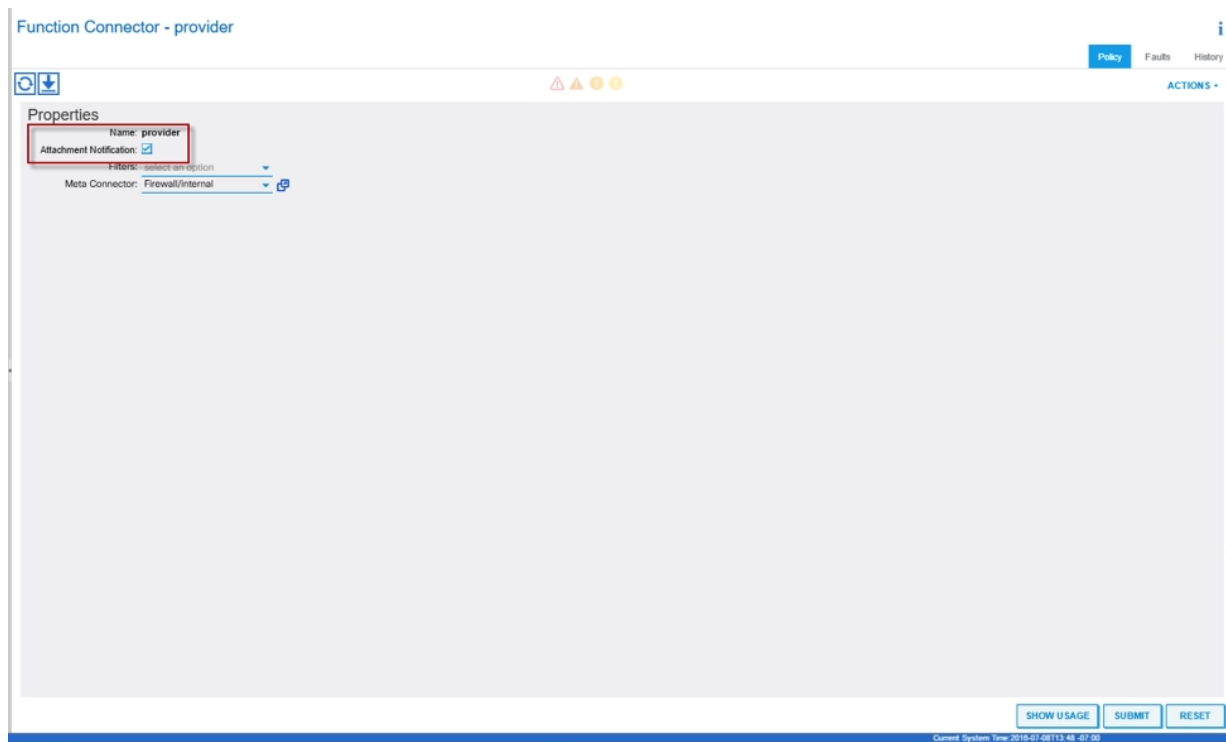
FEATURES AND PARAMETERS

Basic Parameters All Parameters

Meta Folder/Param Key Name Value Mandatory Locked Shared

IPV4 FirewallAddresses	IPV4FWAddressFold...		false	
IPV4 Policy	IPV4FWPolicyFolder		false	
FirewallPolicyRuleID/Number Only - EX: 1.2.1	10		false	
Action/accept/deny/deny-vpn	Action	accept	false	false
Destination Address or VIP	DestAddrVIP		false	false
Incoming interface(internal/externa)	InInterface	internal	false	false
LoggingOptions	Logging		false	false
Name	Name	10	false	false
OrderNo	OrderNo	10	true	false
Outcoming interface(internal/externa)	OutInterface	external	false	false
SecurityProfiles	SecurityProfiles		false	false
Source Address Folder	SrcAddrFolder		false	false
Source Address Name(all :)	SrcAddr	PolicyObjects/IPv4FWAddressFolder/all	false	false
Source Address Group Name(dyn_epg_int_grp)	SrcAddrGrp	PolicyObjects/IPv4FWAddressFolder/dyn_epg_int_grp	false	false
Schedule list name	Schedule	PolicyObjects/ScheduleFolder/always	false	false
Service	Service	PolicyObjects/FWServiceFolder/ALL	false	false
Enable This Policy	Status	enable	false	false
FirewallPolicyRuleID/Number Only - EX: 1.2.1	20		false	false
IPV6 DoS Policy	IPV6DoS-PolicyFolder		false	false
IPV6 FirewallAddresses	IPV6FWAddressFold...		false	

From above example, we added “dyn_epg_int_grp” to **Source Address Group Name** field under Policy 10



From **L4-L7 Service Graph Template>Function Node>Consumer/Provider**, we have to check the box **Attachment Notification** in order for ACI to notify Fortigate when Endpoint attached to the Group.

The screenshot shows the 'EPG - App1' configuration page with the 'Operational' tab selected. The 'Client End-Points' section shows a table with one entry for 'App2'.

End Point	MAC	IP	Learning Source	Hosting Server	Reporting Controller Name	Interface	Multicast Address	Primary VLAN For Micro-Seg	Port Encap (Or Secondary VLAN For Micro-Seg)
App2	00:50:56:B4:ED:2C	15.1.1.20	learned vmm	10.100.11.30	vcenter	Node-101/Fex-101/eth1/1 (learned,vmm)	---	---	vlan-2777

EPG Operational level indicated Endpoint attached to the EPG.

FortiGate 3700D FGT37D4615800597						Interim	admin
Address (34)						By Category	Alphabetically
Name	Type	Details	Interface	Visibility	Ref.		
Adobe Login	Wildcard FQDN	*adobelogin.com	<input type="checkbox"/> any	<input checked="" type="checkbox"/>	1		
Gotomeeting	Wildcard FQDN	*gotomeeting.com	<input type="checkbox"/> any	<input checked="" type="checkbox"/>	1		
SSLVPN_TUNNEL_ADDR1	IP Range	10.212.134.200 - 10.212.134.210	<input checked="" type="checkbox"/> SSL-VPN tunnel interface (ssl5209)	<input checked="" type="checkbox"/>	2		
Windows update 2	Wildcard FQDN	*windowsupdate.com	<input type="checkbox"/> any	<input checked="" type="checkbox"/>	1		
adobe	Wildcard FQDN	*adobe.com	<input type="checkbox"/> any	<input checked="" type="checkbox"/>	1		
all	Subnet	0.0.0.0/0	<input type="checkbox"/> any	<input checked="" type="checkbox"/>	4		
android	Wildcard FQDN	*android.com	<input type="checkbox"/> any	<input checked="" type="checkbox"/>	1		
apple	Wildcard FQDN	*apple.com	<input type="checkbox"/> any	<input checked="" type="checkbox"/>	1		
appstore	Wildcard FQDN	*appstore.com	<input type="checkbox"/> any	<input checked="" type="checkbox"/>	1		
authgfx.ms	FQDN	authgfx.ms	<input type="checkbox"/> any	<input checked="" type="checkbox"/>	1		
autoupdate.opera.com	FQDN	autoupdate.opera.com	<input type="checkbox"/> any	<input checked="" type="checkbox"/>	1		
citrix	Wildcard FQDN	*citrixonline.com	<input type="checkbox"/> any	<input checked="" type="checkbox"/>	1		
dropbox.com	Wildcard FQDN	*dropbox.com	<input type="checkbox"/> any	<input checked="" type="checkbox"/>	1		
dyn_App1_15.1.1.20	Subnet	15.1.1.20/32	<input type="checkbox"/> any	<input checked="" type="checkbox"/>	1		
dyn_Web1_16.1.1.20	Subnet	16.1.1.20/32	<input type="checkbox"/> any	<input checked="" type="checkbox"/>	1		
dyn_epg_addr_none	Subnet	0.0.0.0/32	<input type="checkbox"/> any	<input checked="" type="checkbox"/>	0		
ease	Wildcard FQDN	*ease.com	<input type="checkbox"/> any	<input checked="" type="checkbox"/>	1		
firefox update server	Wildcard FQDN	aus*.mozilla.org	<input type="checkbox"/> any	<input checked="" type="checkbox"/>	1		
fortinet	Wildcard FQDN	*fortinet.com	<input type="checkbox"/> any	<input checked="" type="checkbox"/>	1		
google-drive	Wildcard FQDN	*drive.google.com	<input type="checkbox"/> any	<input checked="" type="checkbox"/>	1		
google-play	FQDN	play.google.com	<input type="checkbox"/> any	<input checked="" type="checkbox"/>	1		
google-play2	Wildcard FQDN	*ggpht.com	<input type="checkbox"/> any	<input checked="" type="checkbox"/>	1		
google-play3	Wildcard FQDN	*books.google.com	<input type="checkbox"/> any	<input checked="" type="checkbox"/>	1		
googleapis.com	Wildcard FQDN	*googleapis.com	<input type="checkbox"/> any	<input checked="" type="checkbox"/>	1		
icloud	Wildcard FQDN	*icloud.com	<input type="checkbox"/> any	<input checked="" type="checkbox"/>	1		
itunes	Wildcard FQDN	*itunes.apple.com	<input type="checkbox"/> any	<input checked="" type="checkbox"/>	1		
live.com	Wildcard FQDN	*live.com	<input type="checkbox"/> any	<input checked="" type="checkbox"/>	0		
microsoft	Wildcard FQDN	*microsoft.com	<input type="checkbox"/> any	<input checked="" type="checkbox"/>	1		
none	Subnet	0.0.0.0/32	<input type="checkbox"/> any	<input checked="" type="checkbox"/>	0		
skype	Wildcard FQDN	*messenger.live.com	<input type="checkbox"/> any	<input checked="" type="checkbox"/>	1		
softwareupdate.vmware.com	FQDN	softwareupdate.vmware.com	<input type="checkbox"/> any	<input checked="" type="checkbox"/>	1		

Fortigate Appended dynamic added Endpoint to the Group.

Supported use scenarios

Physical Fortigate

Go-Through Mode for west-east traffic within data center in ACI.

Scenario: Web server and back-end database servers have same subnet in data center; customer needs firewall service between web server and back-end database servers.

Go-To Mode for north-south traffic for Web Server to access DataBase server in data center.

Scenario: Firewall service for Web Server to access DataBase server in data center.

Virtual Fortigate

Go-Through Mode for west-east traffic within data center in ACI.

Scenario: Web server and back-end database servers have same subnet in data center; customer needs firewall service between web server and back-end database servers.

Go-To Mode for north-south traffic for Web Server to access DataBase server in data center.

Scenario: Firewall service for Web Server to access DataBase server in data center.

Deployment Procedures

Below sections, we will walk through the high level of how to deploy a service insertion as well as detail procedures of how to perform each steps.

Device package installation

To successfully deploy Fortigate Connector into Cisco APIC, customers need to perform the following steps:

1. Import Device Package
2. Add L4-L7 Device
3. Create Functional Profile
4. Create Service Graph Template
5. Deploy Service Graph Template.

Service Deployment

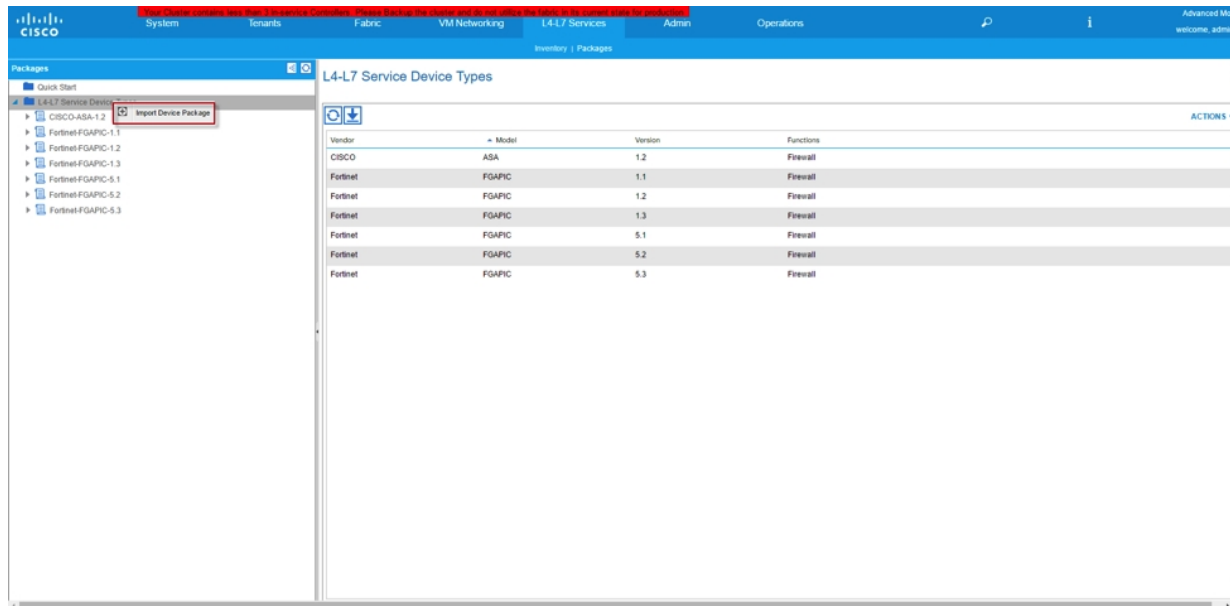
According to the APIC deployment guide, a service device introduces a Layer 4 to Layer 7 service by this typical procedure:

1. Import the device package of the service device,
2. Configure a tenant who asks for network services,
3. Register the device and its logical interfaces,
4. Configure logical device parameters,
5. Configure a layer 3 network,
6. Configure a bridge domain,
7. Configure an application profile,
8. Configure a physical domain (or VMM domain),
9. Configure a VLAN pool,
10. Configure a contract
11. Configure a management endpoint group (EPG),
12. Configure a service graph template,
13. Select default service graph template parameters,
14. Attach the service graph template to a contract
15. Configure additional configuration parameters.

To add a support of a non-Cisco firewall device in the Cisco ACI fabric based data center, a device package should be developed for the APIC. Then the remaining task is standard APIC deployment of a network service device.

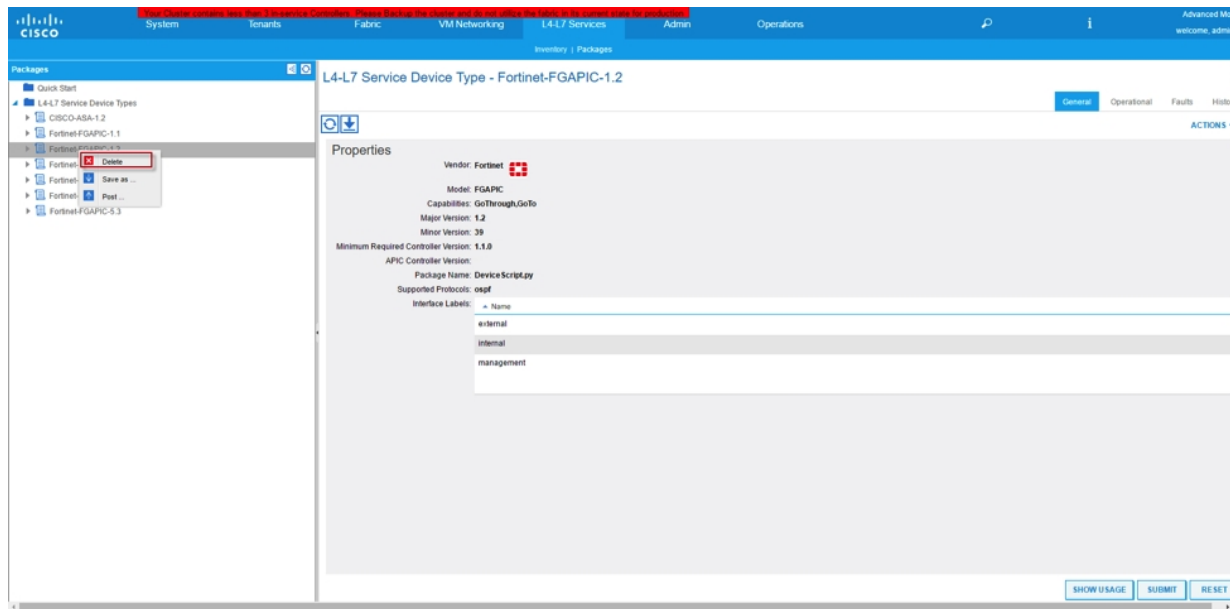
Importing the Device Package

1. Download Device Connector Package from Fortinet Support Web (URL) site to local storage.
2. From APIC menu, Navigate to **L4-L7 Services > Packages** and right click on **L4-L7 Device Type** on the left hand panel. Select **Import Device Package**



Remove Device Package

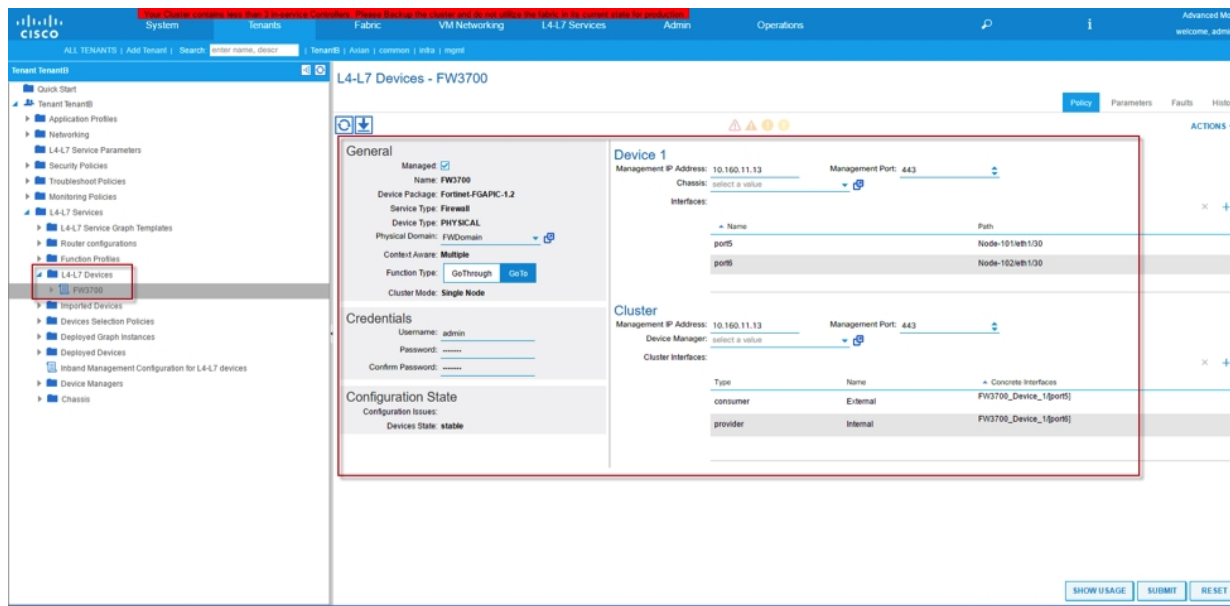
To remove Device Package, navigate to **L4-L7 Services > Packages** and right click on the Device package on the left panel and select **Delete** option.



Basic Steps to add Fortinet Firewall L4-L7 Virtual Device

Add L4-L7 Device

Within Tenant, Expand **L4-L7 Services > L4-L7 Devices**, right click on mouse and select “**Create L4-L7 devices**”



GENERAL

Field	Description / Options
Name	Name of the Device
Device Package	Select Device Package from drop down list
Model	<List of the supported models>
Mode	<ul style="list-style-type: none"> Single Node / HA Cluster
Function Type	<ul style="list-style-type: none"> GoThrough (L2) Goto (L3)

CONNECTIVITY

Field	Description / Options
Physical Domain or VMM Domain	Select from drop down list Domain which you should have configured during APIC Access Policies setup
APIC to Device	<ul style="list-style-type: none"> Out-of-Band In-Band

CREDENTIALS

Field	Description
Username	<login name to the Fortigate>
Password	<Password to login to Fortigate>
Confirm Password	<Password to login to Fortigate>

Device 1

Field	Description / Options
Management IP Address	<IP address to connect to Fortigate>

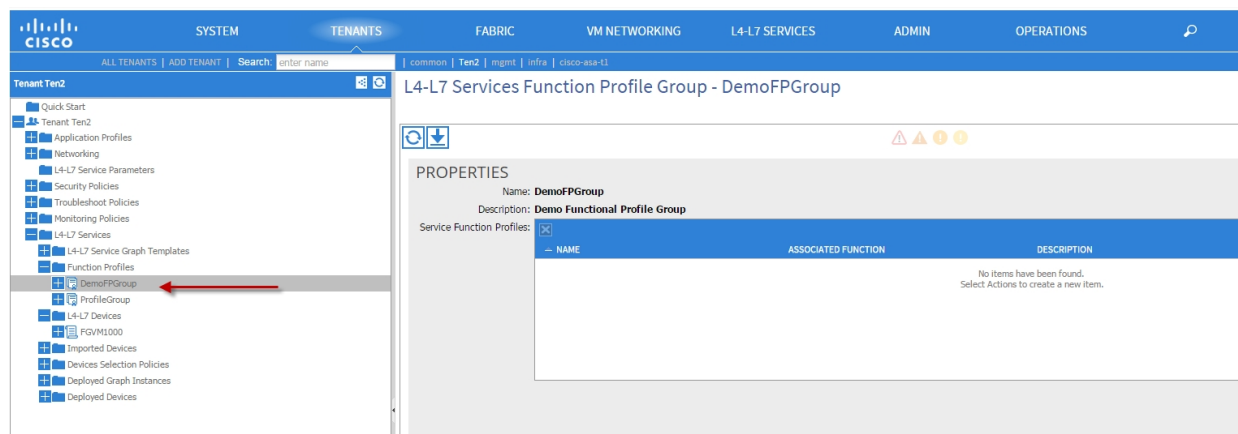
Field	Description / Options
Management Port	<ul style="list-style-type: none"> • http • https <p>https is the prefer method</p>
Connects To	<ul style="list-style-type: none"> • Port (Default), PC, VPC
Physical Interfaces	Click on "+" sign to add interfaces connecting from APIC to FortiGate
Name	<p>Select from Drop down list to select port.</p> <p>(If using Port Channel, please type in the correct Port Channel name ex:PO1, PO2..etc.)</p>

Cluster

Configure all the fields same as Device 1, with exception to Cluster Interface.

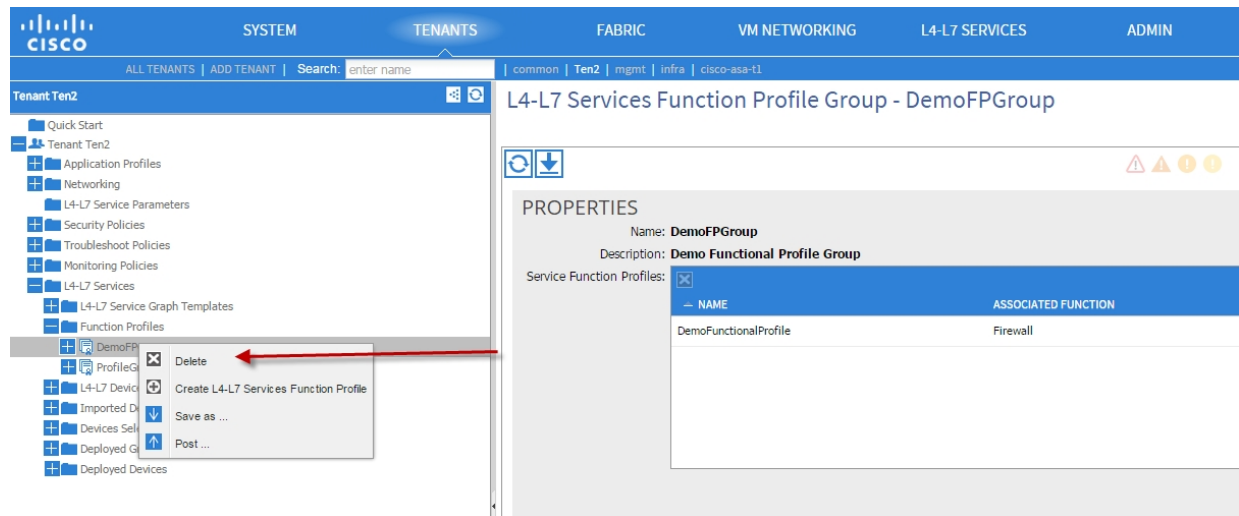
For Cluster Interface, click the "+" icon to add logical device interfaces.

Create Functional Profile Group



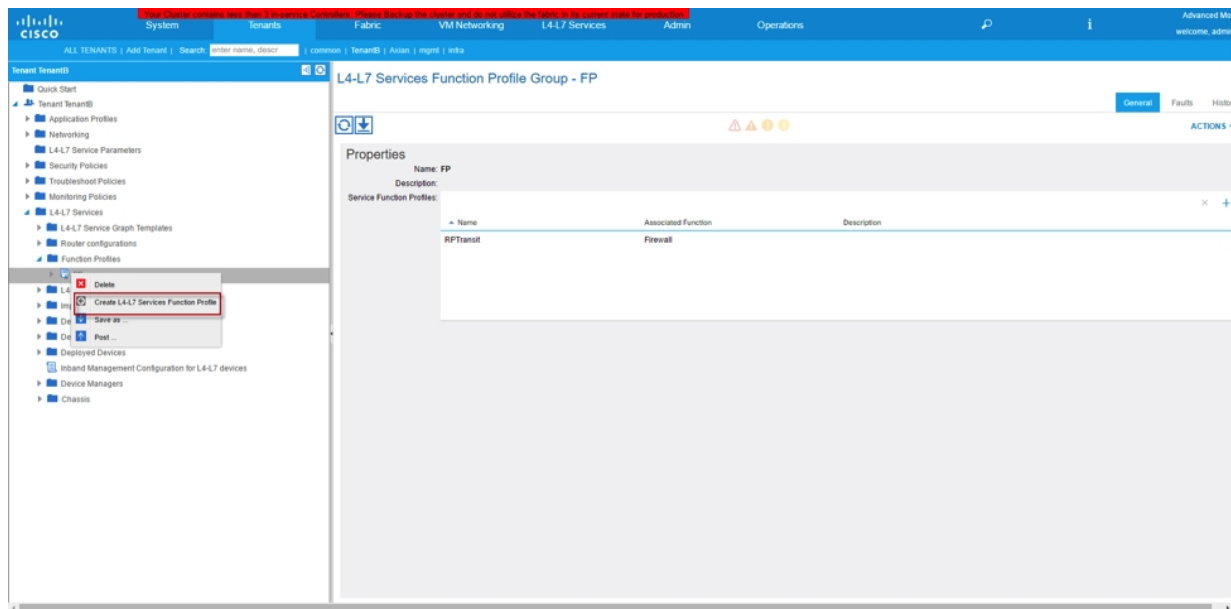
Remove Functional Profile Group

To remove Functional Profile Group, navigate to **Tenant > L4-L7 Services > Functional Profiles** and right click on the Functional Profile group name listed on the left hand panel and select **Delete** option.



Create a Function Profile

Functional Profile defines the template for the Service(s) that is going to deploy such as L4-L7 Device Interface IP addresses, Rule ID, Object Addresses, Policy Rules, Source/Destination Ports...etc.



Functional Profile Objects Explanation under “Features”:

Device Network:

Contained External and Internal Interfaces that will be programmed onto Fortigate VDOM. This is the interfaces (typically external and internal) that will be associated to the VDOM. If user intends to have multiple legs deployment scenario, this is where he/she can add additional interfaces with unique name.



Beginning with FortiGate Connector v1.2, the device package no longer has the option to select VDOM mode and VDOM name. Instead, the VDOM name is automatically generated based on virtual device ID from APIC; the VDOM mode is based selection of Go-to mode and Go-through mode during the device creation. If Go-to mode is selected, user must input IP addresses and subnet mask for each interface; if Go-through mode is selected, user must leave IP address field untouched.

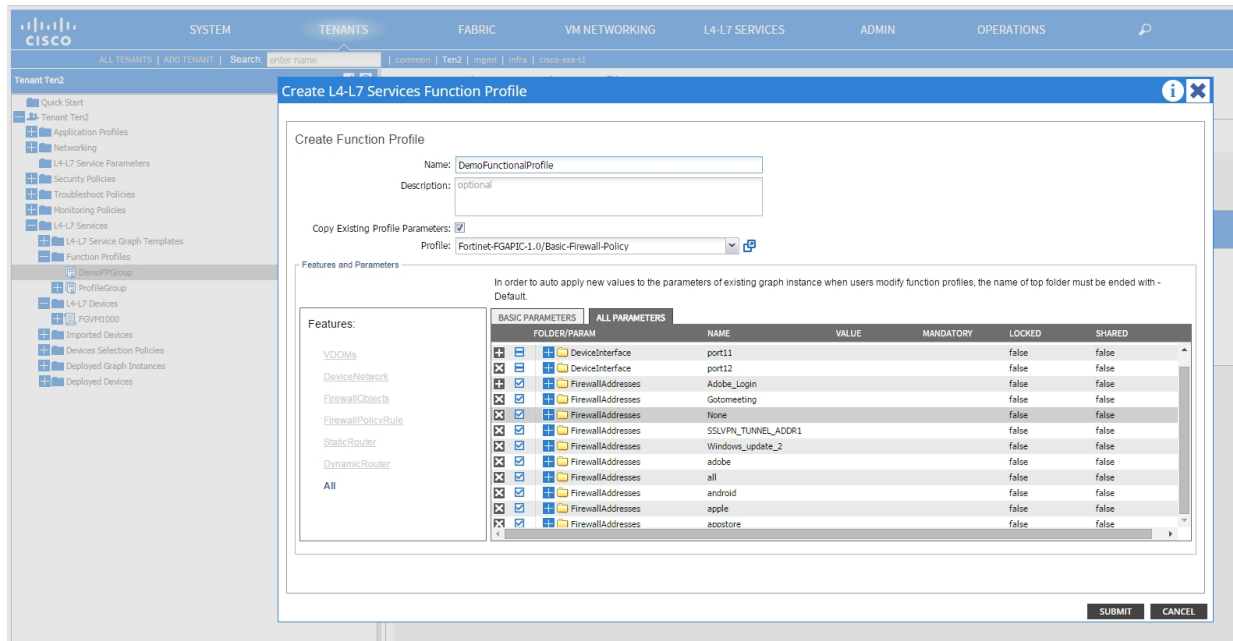
Function Config

Function Config consist of:

- **Network**
 - This field is use for configure Static Routes for IPv4 and IPv6.
- **Policy and Objects**
 - This folder is the container for following list of Folders:
 - a. FWServiceFolder – Firewall Service Object container
 - b. IPv4/IPv6 DoS Policy – Dos Policy configuration
 - c. IPv4/IPv6 FirewallAddresses – Firewall Addresses Object container
 - d. IPv4 Policy – Firewall Policy Rule container
 - e. IPv4 FirewallAddresses Group – Group folder for “Dynamic EPG” feature
 - f. ScheduleFolder – Schedule container
- **VDOM-Folder**
 - VDOM internal and external interfaces

Review

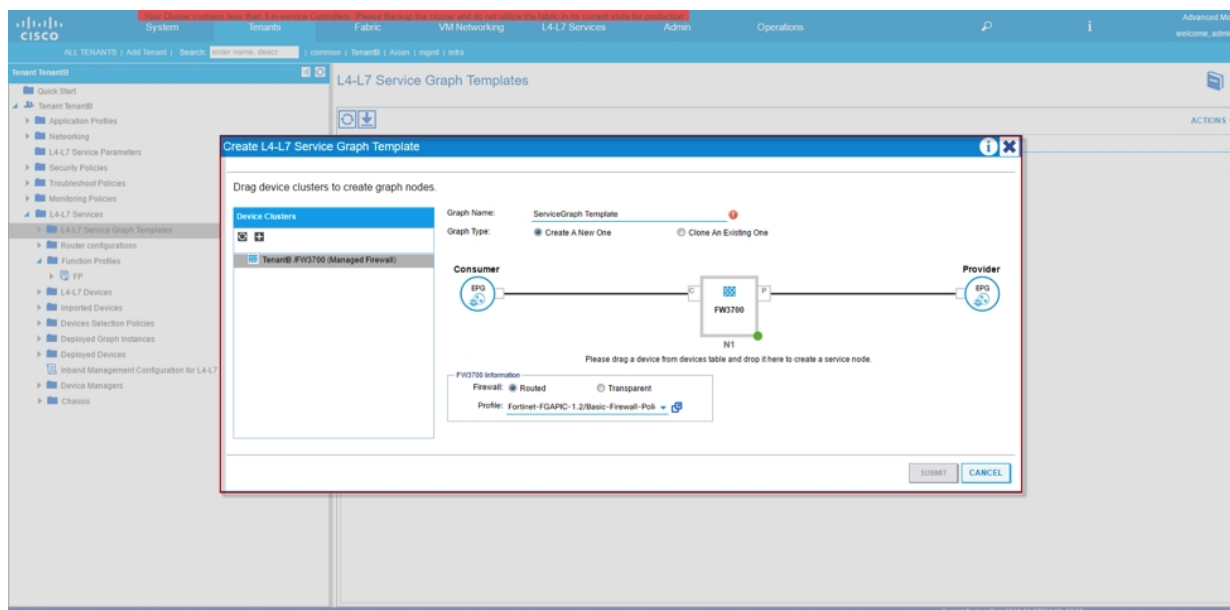
All Field display all the fields in the features listing. If you are satisfy with all your inputs, then hit the submit button to complete your creation of Functional Profile template.



Service Graph

Create Service Graph

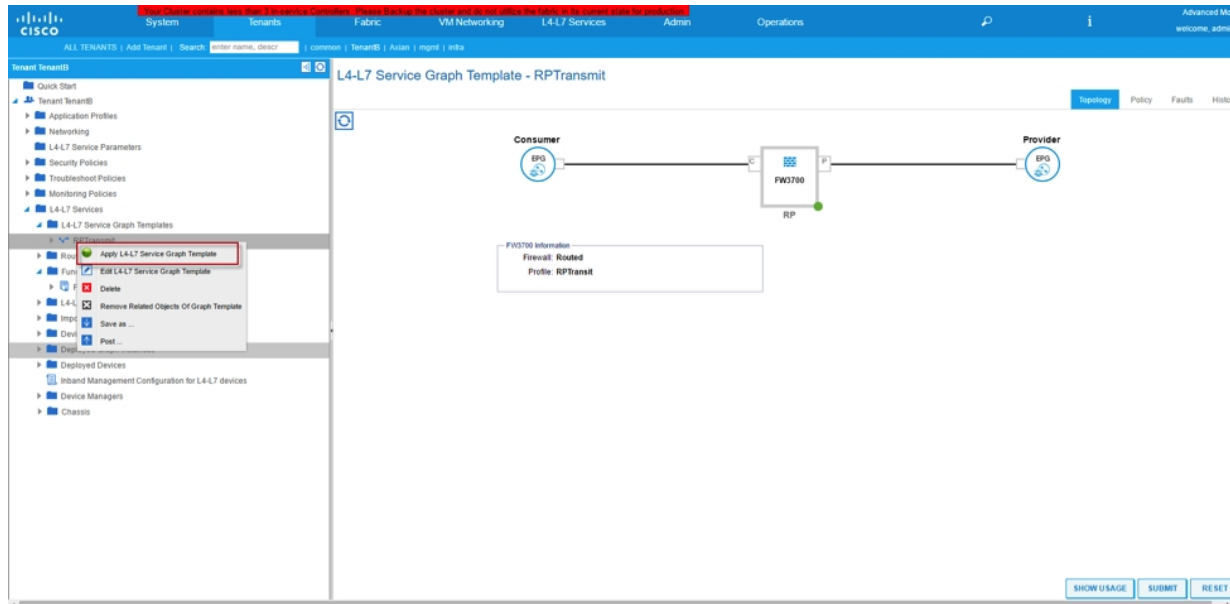
Service Graph template is used to tightly coupled the Functional Profile or Firewall configuration and combine with the Firewall device we defined at earlier steps.



Right Click on **L4-L7 Service Graph Template** to create a Service Graph.

Deploy Service Graph

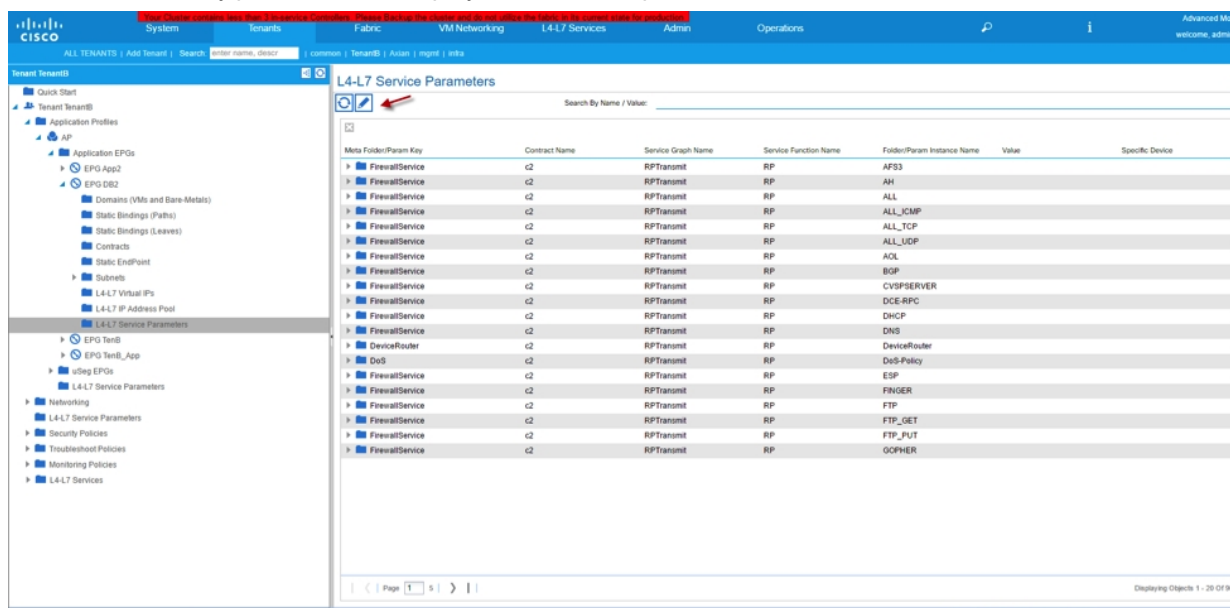
Once we combined the Firewall configuration and associated device together, we are ready to deploy the service Graph to create a VDOM automatically.



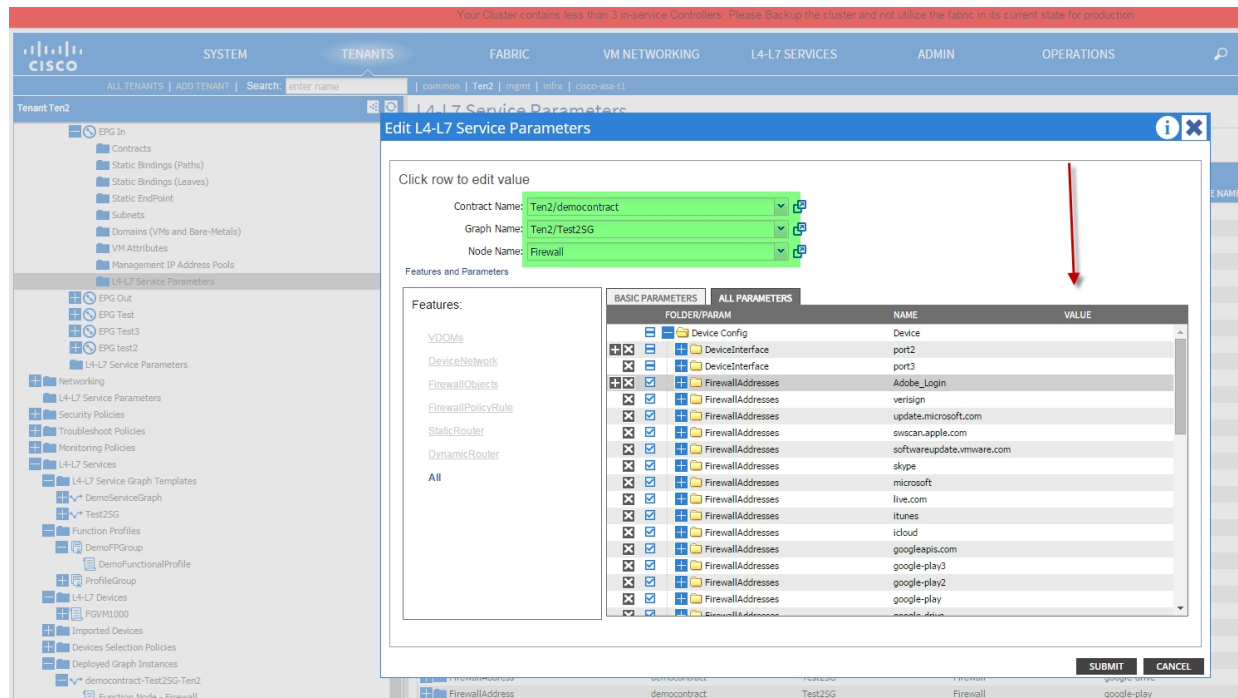
Right Click on Service Graph defined from above and select **Apply L4-L7 Service Graph Template**.

Modify Service Graph

1. From **Tenant>Provider EPG>L4-L7 Service Parameters** and select the pen icon, which will lead you into edit mode to modify parameters on deployed Service Graph.

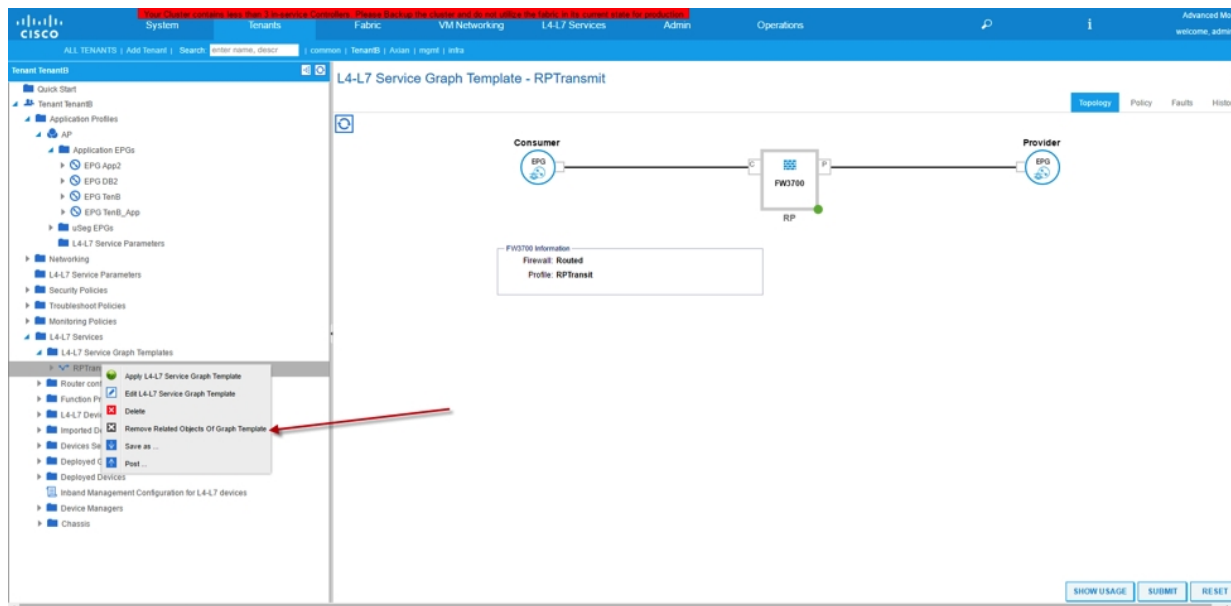


2. On the next screen, select the Contract name, Graph Name and Node name from the drop down list and all the associated Service Graph Parameters will be displayed.
3. Expand the field you want to make modification and change the appropriate value from the drop down list and then hit submit.



Remove Service Graph

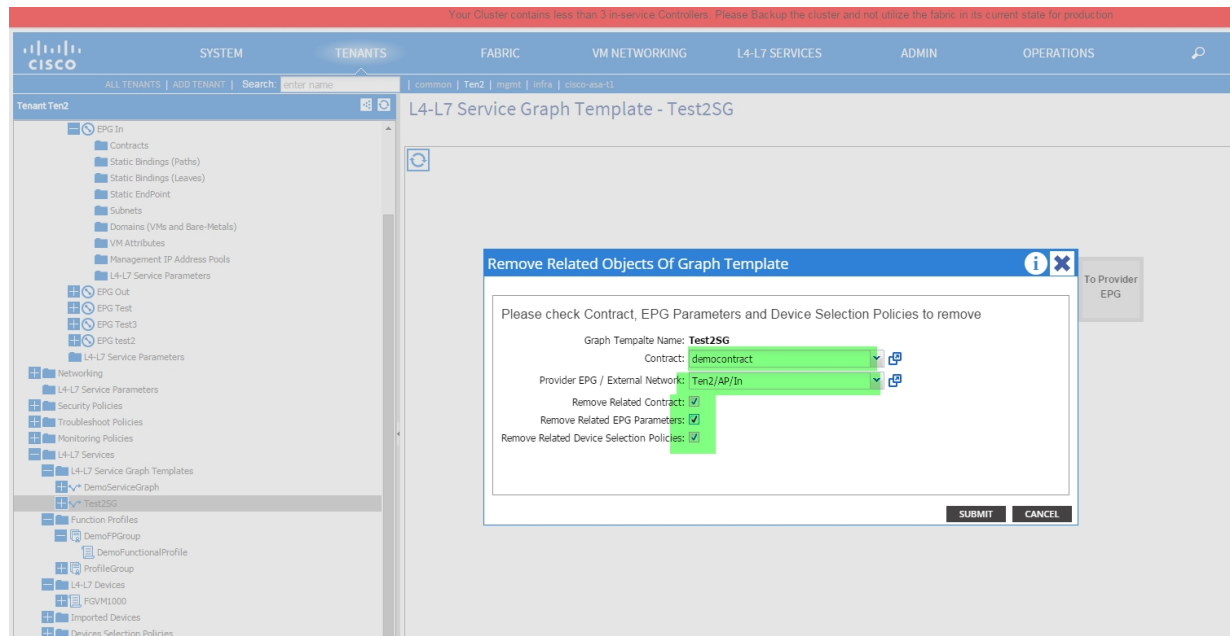
1. Navigate to **Tenant>L4-L7 Services>L4-L7 Service Graph Templates**. Right click on Service Graph template and select **Remove Related Objects Of Graph Template**.



2. Select **Contract and Provider EPG** from the drop down list and check all 3 boxes:

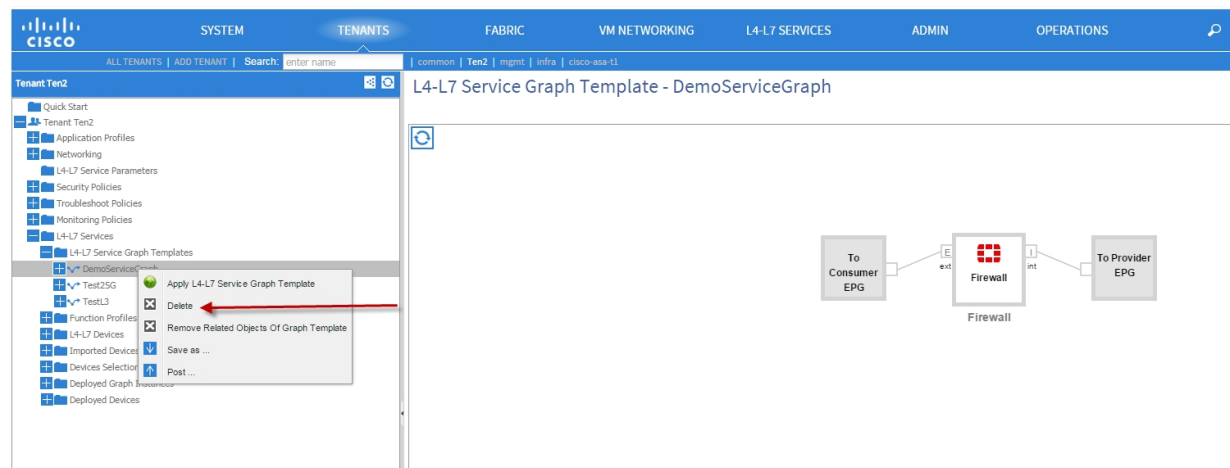
- **Remove Related Contract**
- **Remove Related EPG Parameters**
- **Remove Related Device Selection Policies**

Hit **Submit**. This will remove all the related objects for this Service Graph.



Delete the Service Graph

1. To delete the Service Graph Template, navigate to **Tenant > L4-L7 Services > L4-L7 Service Graph Templates**.
2. Right click on template name listed on the left hand panel and select **Delete** option.



Service Graph deployed

Once the service graph is deployed, the Fortigate device will receive configuration through REST API commands from the Cisco APIC. Below figure shows a successful service graph deployment. The Interface configuration such as vlan, IP..etc and firewall policies are all being programmed onto the Fortigate. From this point forward, any update is continue to be manage by Cisco APIC until the service graph is remove.

The screenshot displays the Cisco APIC GUI for configuring a Function Node - RP. The left sidebar shows the navigation tree with 'Deployed Graph Instances' highlighted. The main panel displays the 'Properties' section for the 'RP' function node, including cluster interfaces and function connectors. The 'Folders And Parameters' section shows a list of parameters for the 'Device Config' folder.

Folder	Parameter Name	Value	Override Name/Value To
Device Config	DeviceInterface	external	epg
	DeviceInterface	internal	epg
Function Config	DeviceRouter	DeviceRouter	epg
	DevS	DevS-Policy	epg
FirewallAddresses	all	all	epg
	auth	auth-gh.ms	epg
FirewallAddresses	auth	auth-gh.ms	epg
	authupdate	authupdate.opera.com	epg

Installation Variations

Deploying Data Center Layer 2 Segmentation with Cisco ACI and FortiGate

Pre-requisites

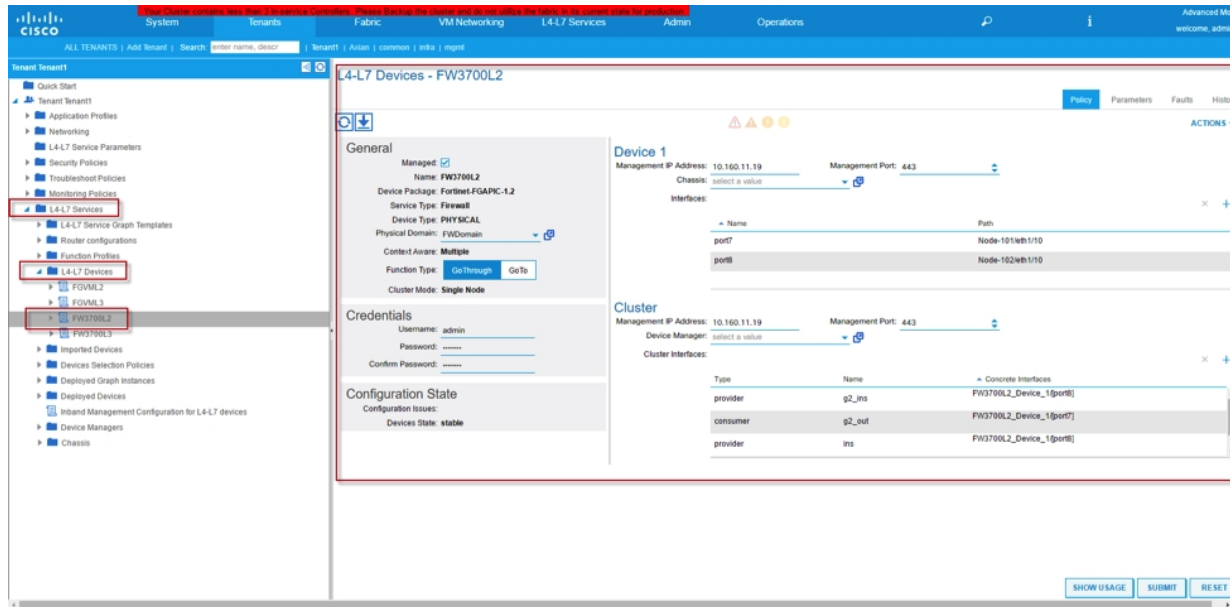
- Fabric Access Policies creation relating to
 - Vlan Pools
 - Domain
 - Attachable Access Entity Profiles
 - Interface Policies
 - Switch policies
- Create Tenant, VRF, 2 Bridge Domains, 2 EPGs
- Associate 2 Bridge Domains to VRF
- Associate 2 EPGs to the 2 Bridge Domains
- Layer 4-7 Device Package has imported into Cisco APIC

Work Flow

1. Create L4-L7 Device with Go-through Mode
2. Create Functional Profile
3. Create Service Graph Template
4. Deploy Service Graph

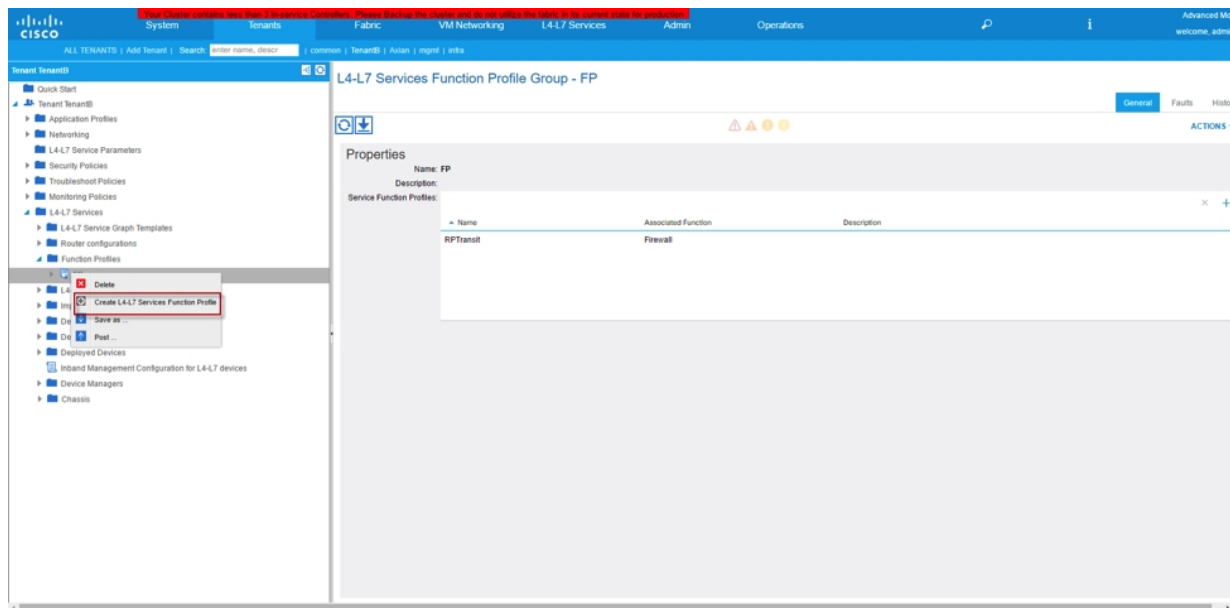
Configuration

Create L4-L7 Device with Go-Through mode on Cisco APIC



Create Functional Profile

Functional Profile defines the template for the Service(s) that is going to deploy, such as L4-L7 Device Interface IP addresses, Rule ID, Object Addresses, Policy Rules, Source/Destination Ports...etc.



Functional Profile Objects Explanation:

Device Config

Contained External and Internal Interfaces that will be programmed onto Fortigate VDOM. These are the interfaces (typically external and internal) that will be associated to the VDOM. If user intends to have multiple legs deployment scenario, this is where additional interfaces with unique names can be added.



User must leave IP address field untouched in Go-through mode.

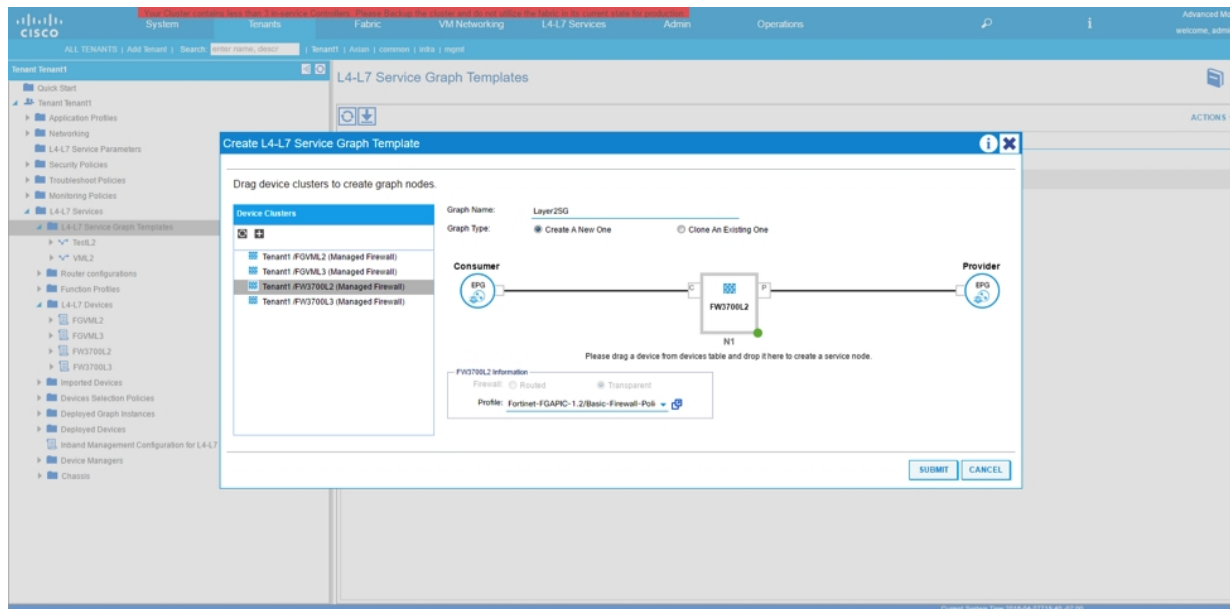
Function Config

Function Config consist of:

- **Network**
 - This field is use for configure Static Routes for IPv4 and IPv6.
- **Policy and Objects**
 - This folder is the container for following list of Folders:
 - a. FWServiceFolder – Firewall Service Object container
 - b. IPv4/IPv6 DoS Policy – Dos Policy configuration
 - c. IPv4/IPv6 FirewallAddresses – Firewall Addresses Object container
 - d. IPv4 Policy – Firewall Policy Rule container
 - e. IPv4 FirewallAddresses Group – Group folder for “Dynamic EPG” feature
 - f. ScheduleFolder – Schedule container
- **VDOM-Folder**
 - VDOM internal and external interfaces

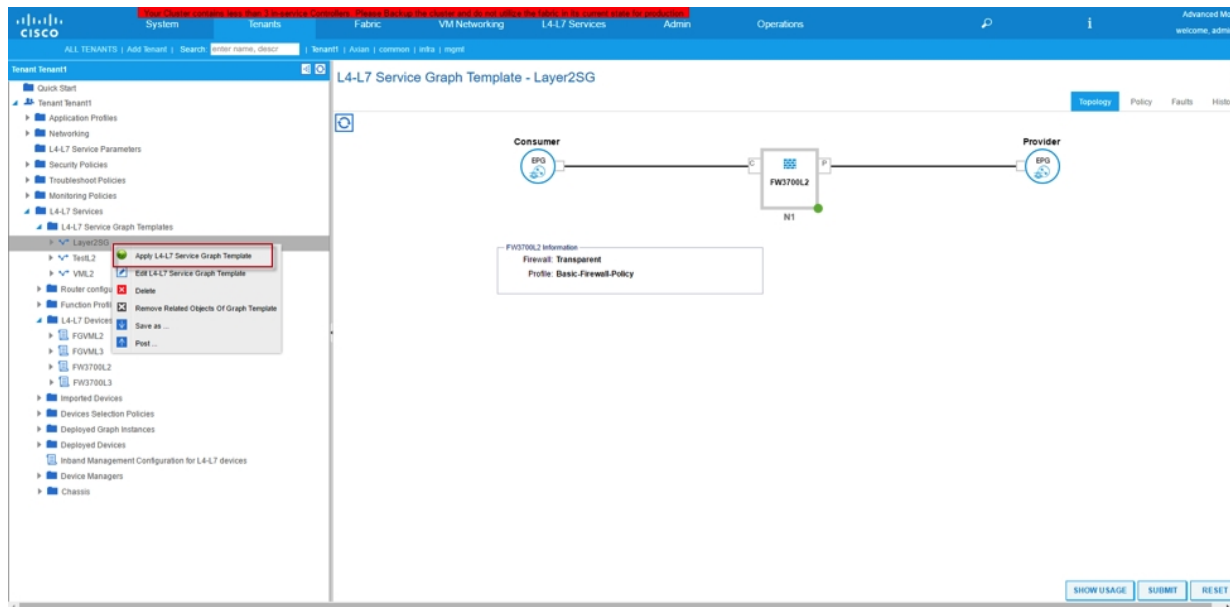
Create Service Graph

Service Graph template is used to tightly coupled the Functional Profile or Firewall configuration and combine with the Firewall device we defined at earlier steps.

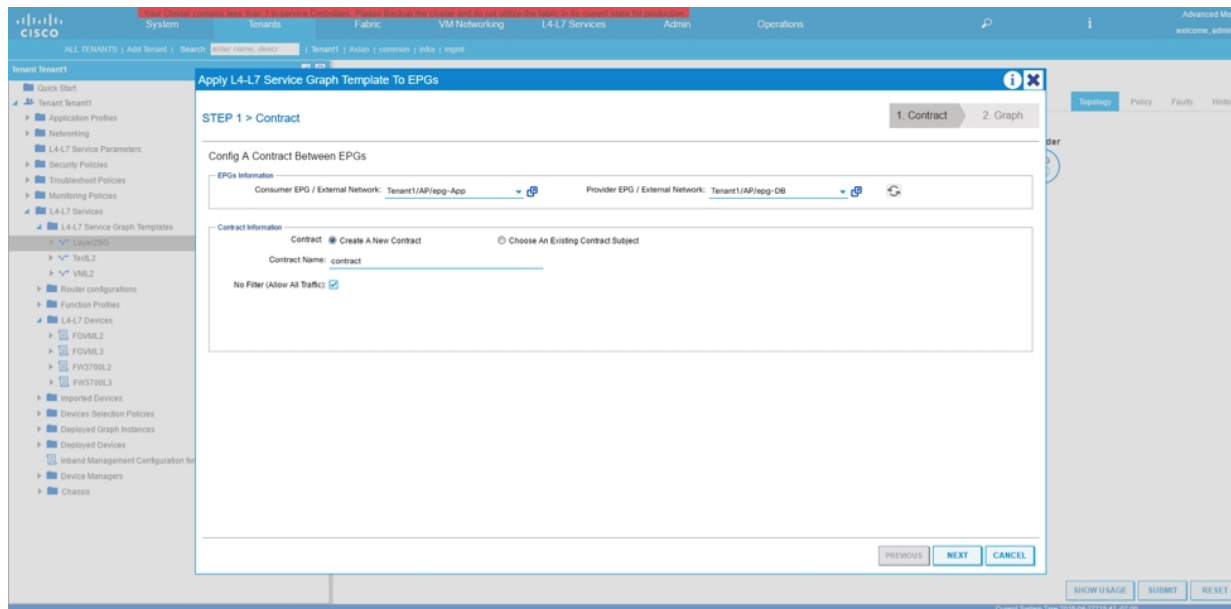


Deploy Service Graph

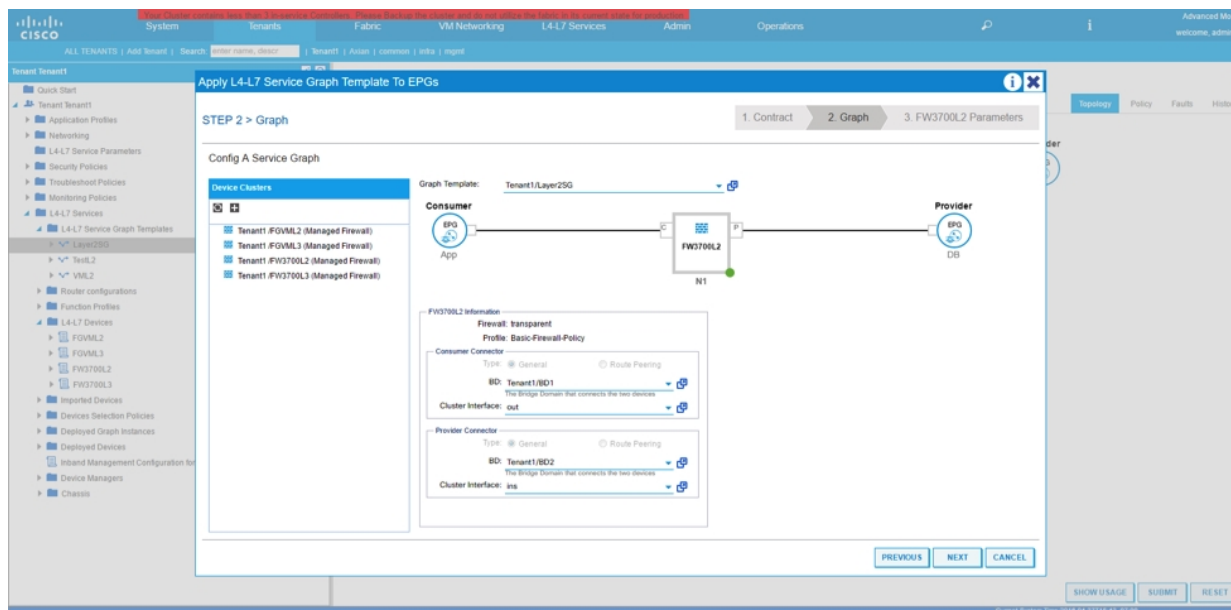
Once we combined the Firewall configuration and associated device together, we are ready to deploy the Service Graph.



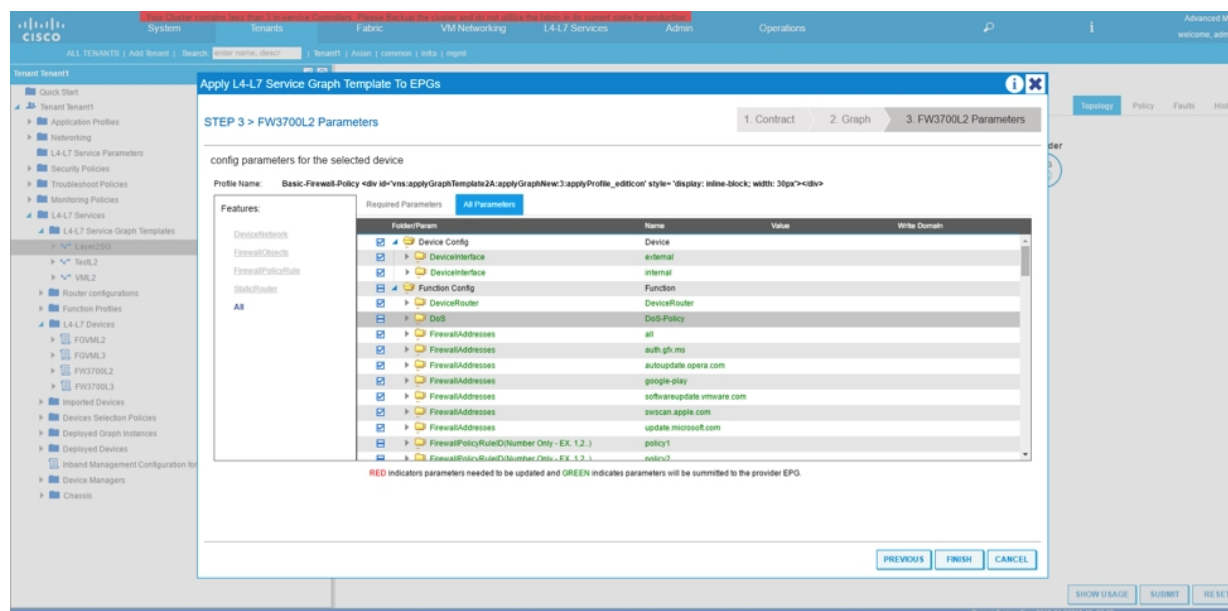
On next screen select the Consumer and Provider EPGs and assign a contract name or select a pre-define contract.



Next screen select the logical interfaces defined during the creation of L4-L7 Device.

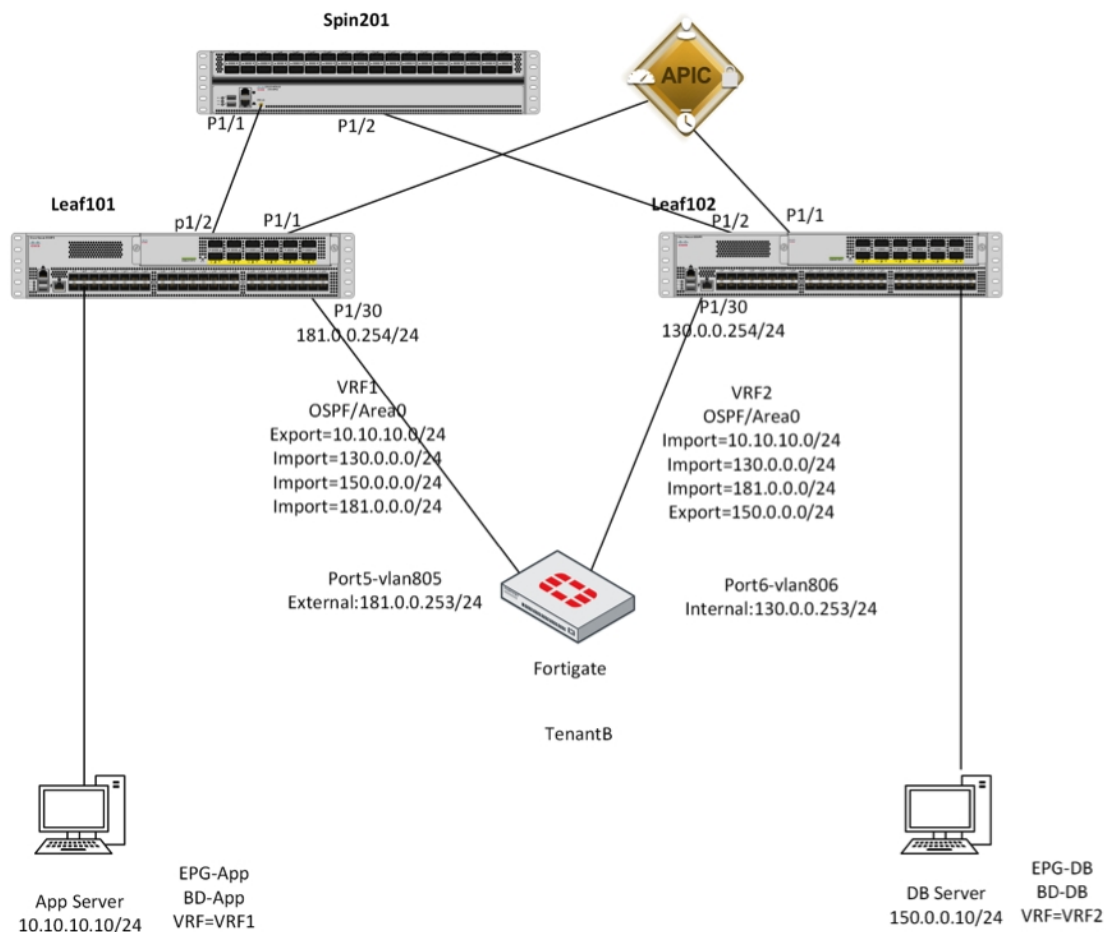


Next screen is the last minute to validate all configurations before deploy, then hit the submit button.



Deploying Data Center Layer 3 Segmentation with Cisco ACI and FortiGate

L3 Segmentation Topology



Introduction

This document describes the configuration walk through of L4-L7 Service Graph with L3 Segmentation within Data Center.

Prerequisites

Please pre-configure below configuration before deploying this design:

- Fabric Access Policies creation relating to:
 - VLAN Pools
 - Domain

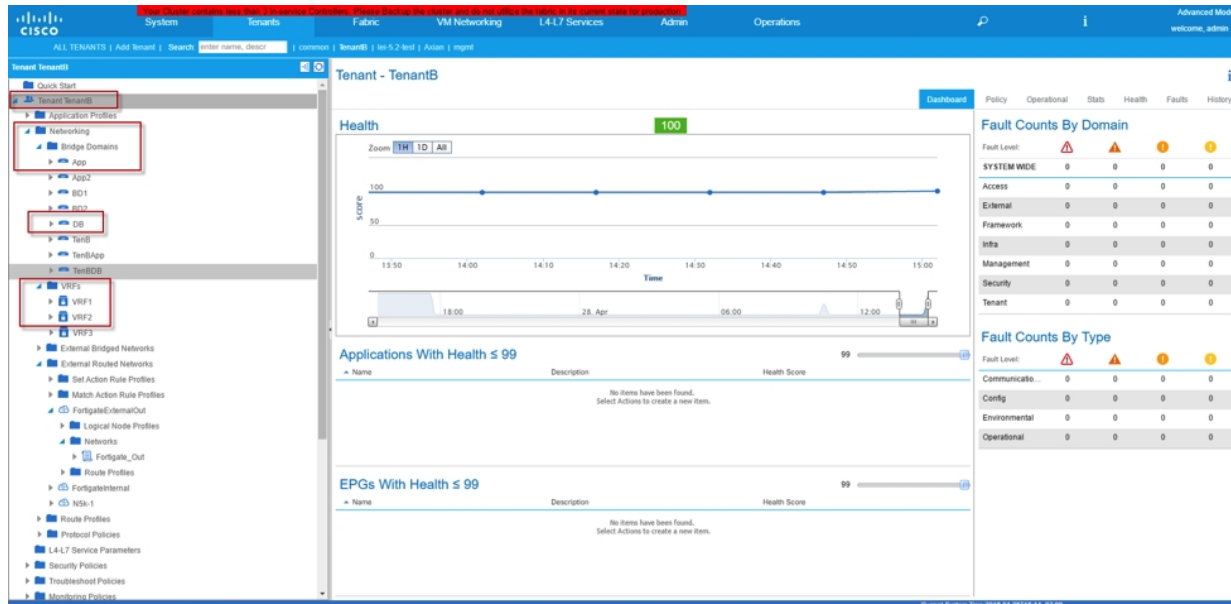
- Attachable Access Entity Profiles
- Interface Policies
- Switch Policies
- L4-L7 Device Package has imported into Cisco APIC

Work Flow

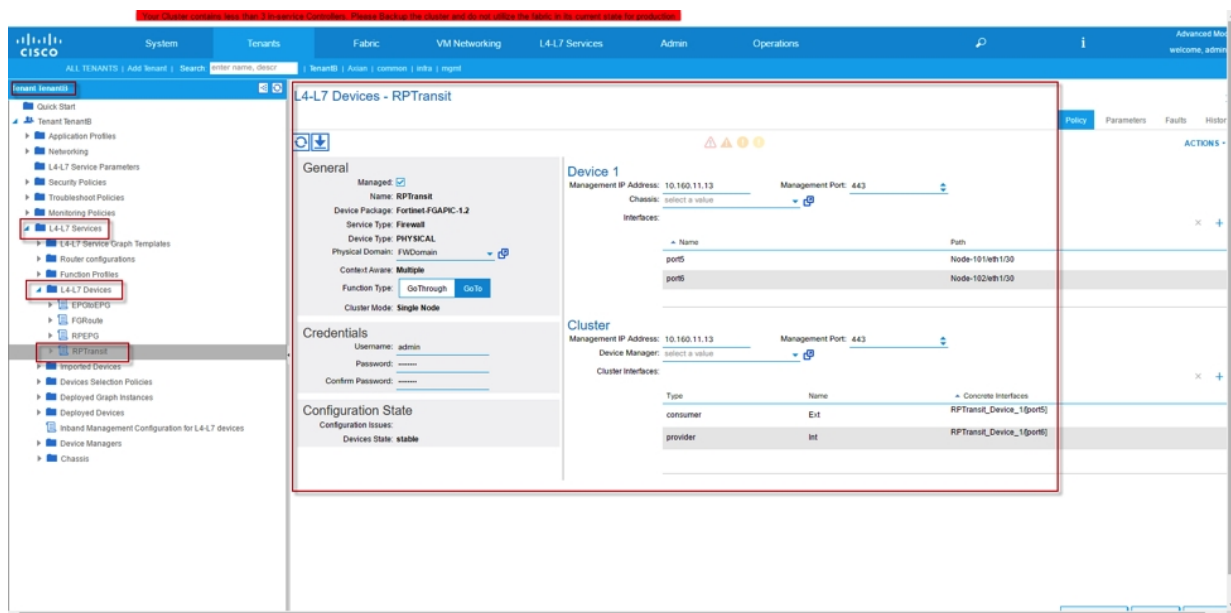
1. Create Tenant (TenantB in our example)
2. Create VRFs (VRF1 and VRF2 in our example)
3. Create Bridge Domains and map to VRFs (Bridge Domain App and DB are mapped to VRF1 and VRF2 respectively in our example)
4. Create EPGs and map to Bridge Domains (EPG-DB and EPG-App in our example)
5. Create two L3Out EPGs (1 for Firewall External and 1 for Firewall Internal. In our example, we created "FortigateExternalOut" for Firewall External and "FortigateInternal" for Firewall Internal)
6. Configure gateway IPs on Bridge Domains (DB and App) for App and DB Servers
7. Ensure "Unicast Routing" is checked in each Bridge Domain
8. In Bridge Domain App, associate L3Outs to "FortigateExternalOut"; in Bridge Domain DB, associate L3Outs to "FortigateInternal"
9. Map App and DB machines to EPGs and configure correct IP addresses, and use Bridge Domain IP address (configured in step 6) as its gateway
10. Verify App and DB machines can ping to gateway IP address
11. Create L4-L7 Device with GoTo mode
12. Create Functional Profile Group as well as Functional Profile
13. Create Route Profiles
14. Create L4-L7 Service Graph Template
15. Deploy L4-L7 Service Graph

Configuration

Configure the Bridge Domain DB and App as well as VRF1 and VRF2. Associate Bridge Domain App to VRF1 and Bridge Domain DB to VRF2.



Configure L4-L7 Device for physical Fortigate (GoTo Mode)



Configure L3Out for Fortigate External Interface and associate with VRF1

Properties

Tags:

Label:

Target DSCP: unspecified

Route Control Enforcement: ☐ Import ☐ Export

VRF: TenantB/VRF1

Resolved VRF: TenantB/VRF1

External Routed Domain: Internet

Route Profile for Interleaf: select a value

Route Control For Dampening:

Address Family Type:

Route Dampening Policy:

Enable BGP/EGRP/OSPF: ☐ BGP ☒ OSPF

OSPF Area ID: 0

OSPF Area Cost: 1

OSPF Area Type: NSSA area ☒ Regular area ☐ Stub area

OSPF Area Cost: 1

SHOW USAGE SUBMIT RESET

Configure SVI for L3Out Fortigate External out

, ND policy: select a value, Egress Data Plane Policing Policy: select a value, Ingress Data Plane Policing Policy: select a value, and a table for 'Routed Interfaces' with one entry: Path: Node-101eth1/00, IP Address: 181.0.0.254/24, Side A IP: , Side B IP: , MAC Address: 00:22:8D:F8:19:FF, MTU (Bytes): 9000, Encap: vlan-805."/>

Properties

Name: ExternalIP

Description: optional

Label:

ND policy: select a value

Egress Data Plane Policing Policy: select a value

Ingress Data Plane Policing Policy: select a value

Routed Interfaces:

Path	IP Address	Side A IP	Side B IP	MAC Address	MTU (Bytes)	Encap
Node-101eth1/00	181.0.0.254/24	<input type="text"/>	<input type="text"/>	00:22:8D:F8:19:FF	9000	vlan-805

Routed Sub-Interfaces:

Path	IP Address	MAC Address	MTU (Bytes)	Encap
No items have been found. Select Actions to create a new item.				

Configure Route ID for L3Out Fortigate External Out

The screenshot shows the Cisco ACI GUI with the 'Logical Node Profile - ExternalNP' configuration page. The left sidebar shows the navigation tree with 'Logical Node Profiles' selected. The main panel displays the 'Properties' section for 'ExternalNP'. The 'Nodes' table is highlighted with a red box, showing the following data:

Node ID	Router ID	Static Routes	Endpoint Address
tpology005-1node-101	101.0.0.105		101.0.0.105

Buttons at the bottom right include 'SHOW USAGE', 'SUBMIT', and 'RESET'.

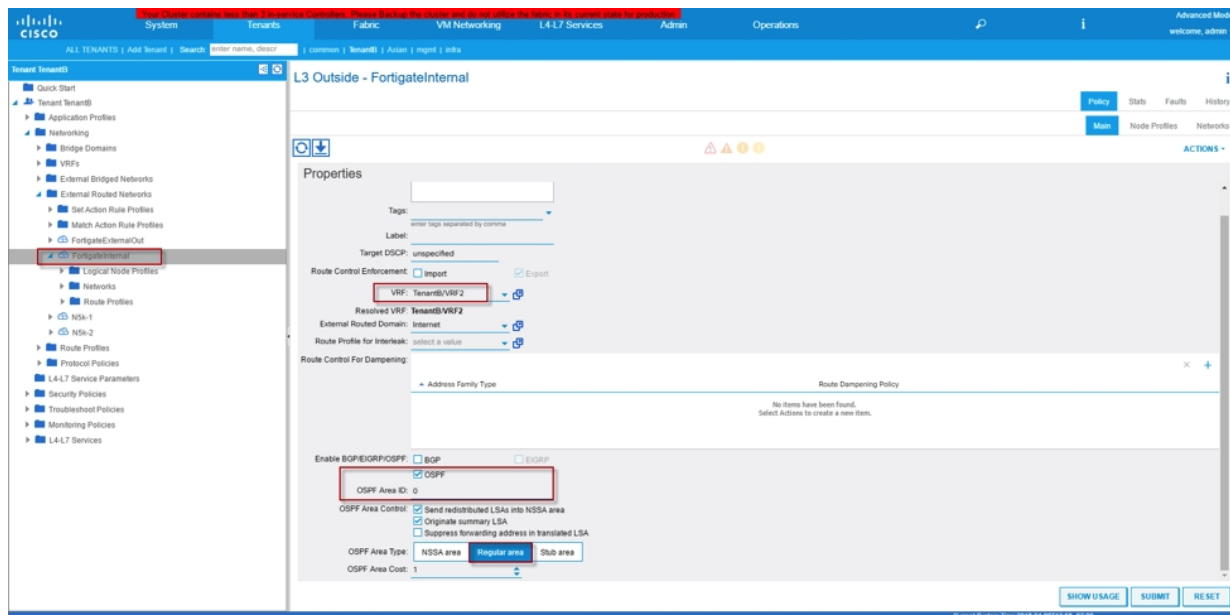
Configure Import/Export Route Control on Subnets for Fortigate External out

The screenshot shows the Cisco ACI GUI with the 'External Network Instance Profile - Fortigate_Out' configuration page. The left sidebar shows the navigation tree with 'External Network Instance Profiles' selected. The main panel displays the 'Properties' section for 'Fortigate_Out'. The 'Subnets' table is highlighted with a red box, showing the following data:

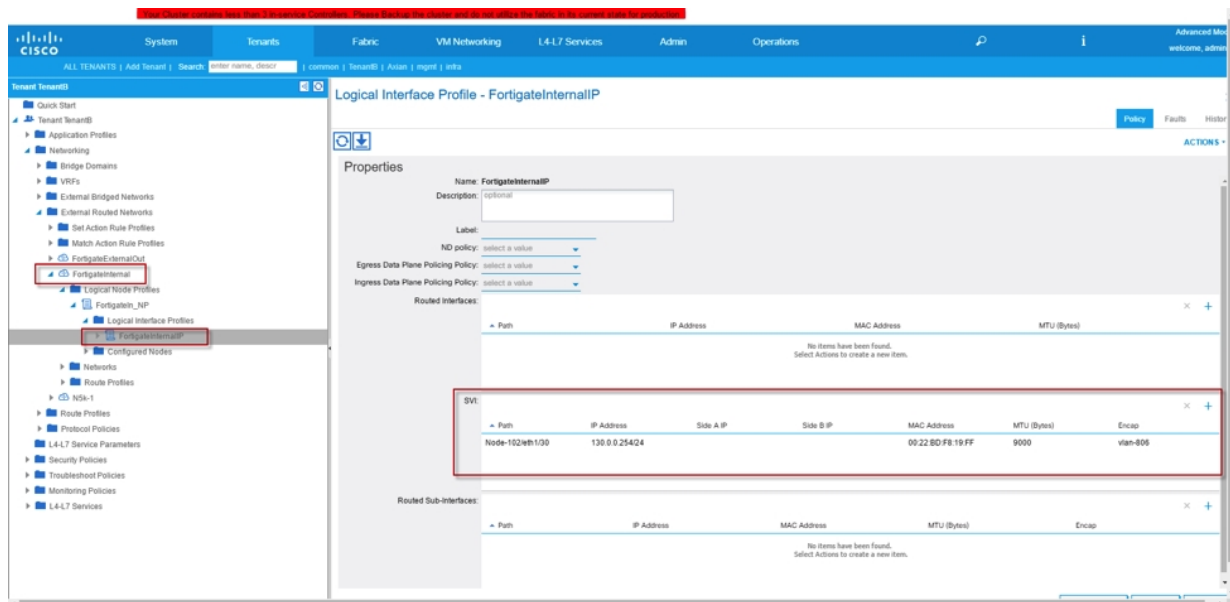
IP Address	Scope	Aggregate	Route Control Profile	Route Summarization Policy
10.10.10.0/24	Export Route Control Subnet			
130.0.0.0/24	External Subnets for the External EPG			
150.0.0.0/24	External Subnets for the External EPG			
181.0.0.0/24	External Subnets for the External EPG			
192.168.1.0/30	Export Route Control Subnet			

Buttons at the bottom right include 'SHOW USAGE', 'SUBMIT', and 'RESET'.

Configure L3Out for Fortigate Internal and associate with VRF2



Configure SVI for L3Out Fortigate Internal



Configure Route ID for L3Out Fortigate Internal

The screenshot shows the Cisco ACI GUI for configuring a Logical Node Profile. The left sidebar shows the navigation tree with 'FortigateInternal' selected. The main panel displays the 'Logical Node Profile - FortigateInternal_NP' configuration. The 'Properties' section includes fields for Name, Description, Label, and Target DSCP. The 'Nodes' table is highlighted with a red box, showing the following data:

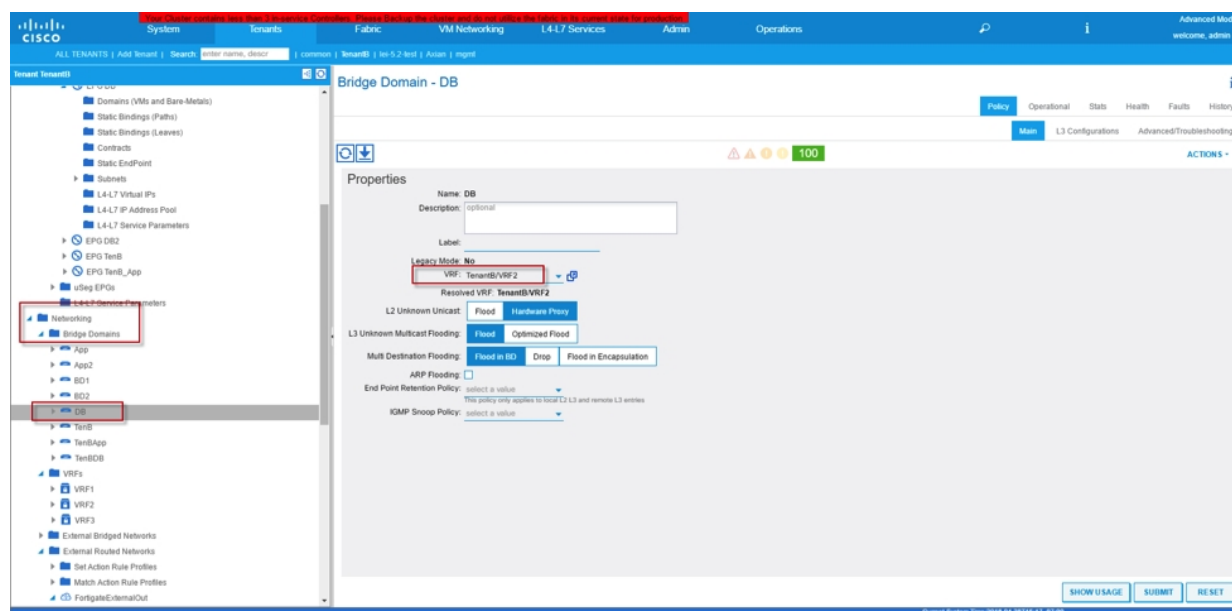
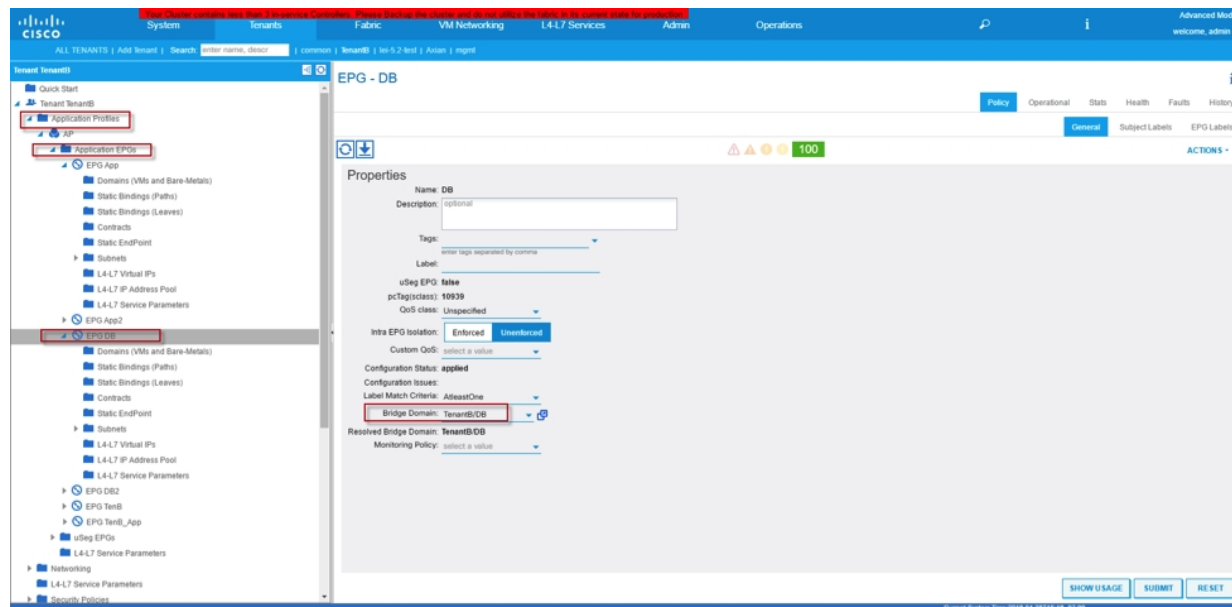
Node ID	Router ID	Static Routes	Loopback Address
topology/pod-1-node-102	102.0.0.105		102.0.0.105

Configure Import/Export Route Control on Subnet for L3Out Fortigate Internal

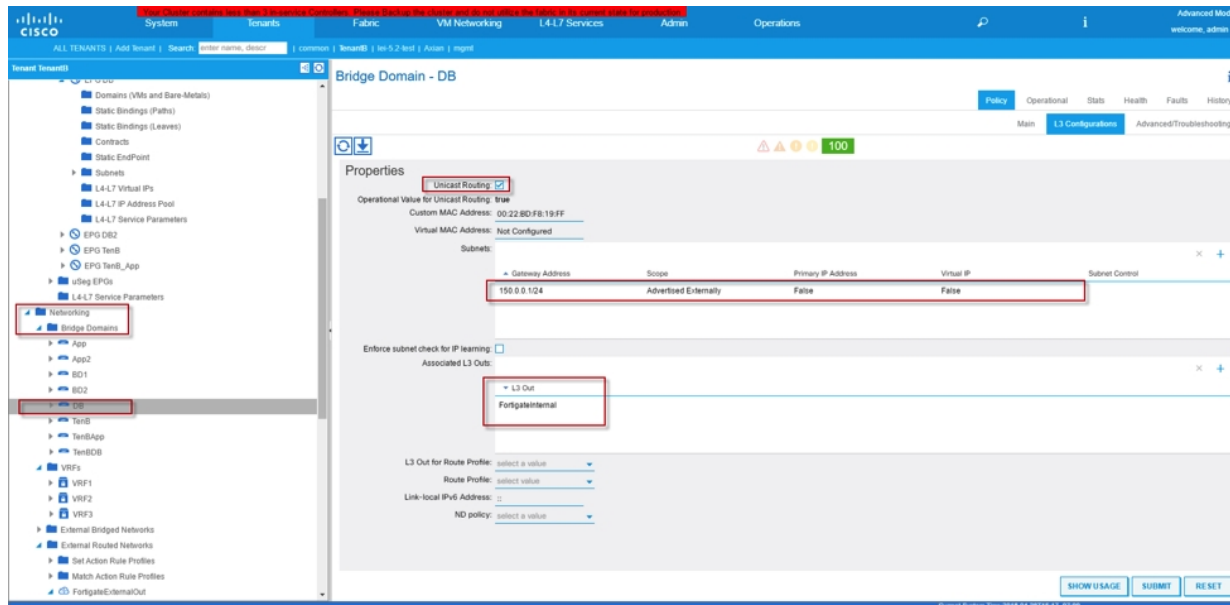
The screenshot shows the Cisco ACI GUI for configuring an External Network Instance Profile. The left sidebar shows the navigation tree with 'FortInternal' selected. The main panel displays the 'External Network Instance Profile - FortInternal' configuration. The 'Properties' section includes fields for Name, Tags, Description, Configured VRF name, Resolved VRF, Target DSCP, and Configuration Status. The 'Route Control' table is highlighted with a red box, showing the following data:

IP Address	Scope	Aggregate	Route Control Policy	Route Summarization Policy
10.10.10.0/24	External Subnets for the External EPG			
130.0.0.0/24	External Subnets for the External EPG			
150.0.0.0/24	Export Route Control Subnet			
181.0.0.0/24	External Subnets for the External EPG			
192.168.1.0/24	External Subnets for the External EPG			

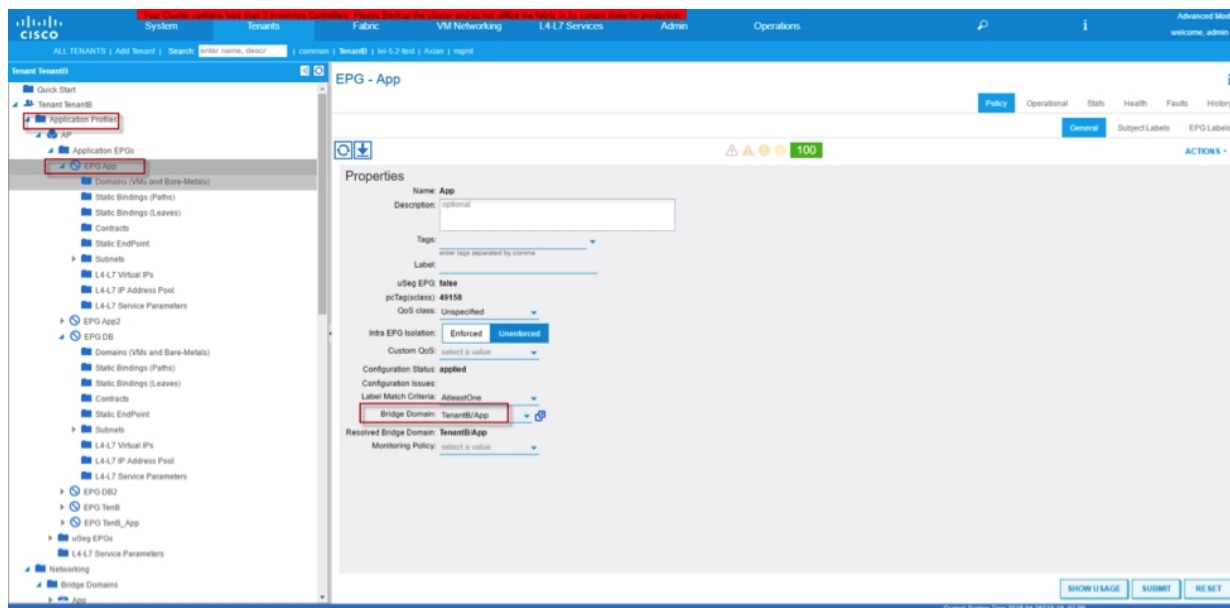
Associate EPG “DB” to Bridge Domain “DB” and attach Bridge Domain to VRF2

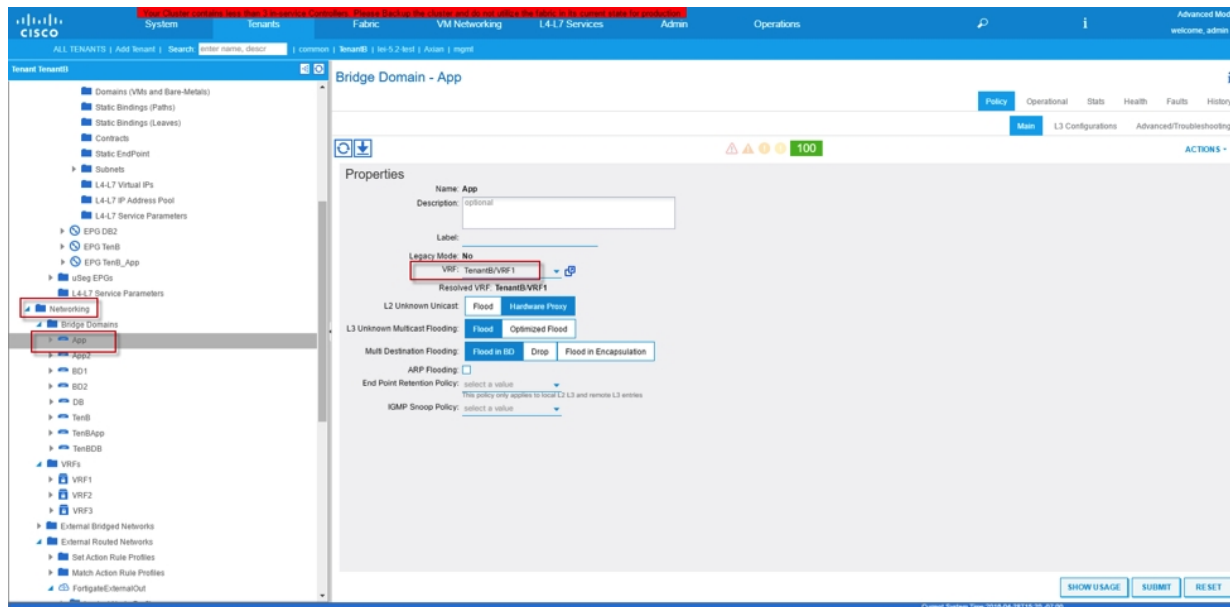


Configure Bridge Domain with Unicast Routing, assign SVI and associate L3Out to “FortigateInternal”

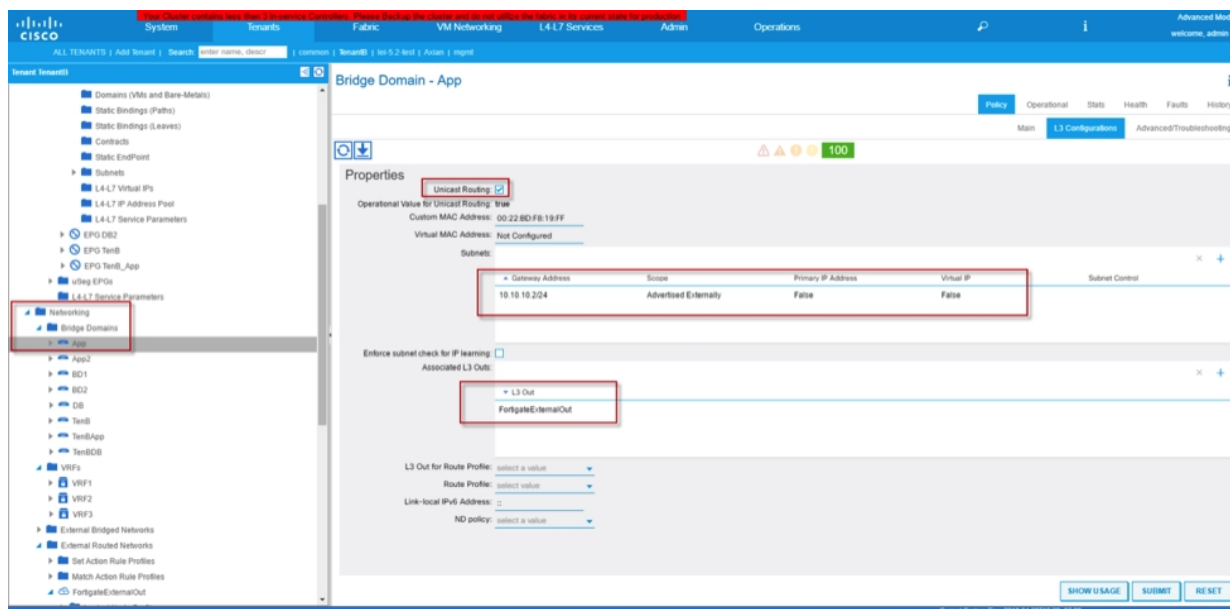


Associate EPG “App” to Bridge Domain “App” and attach Bridge Domain to VRF1

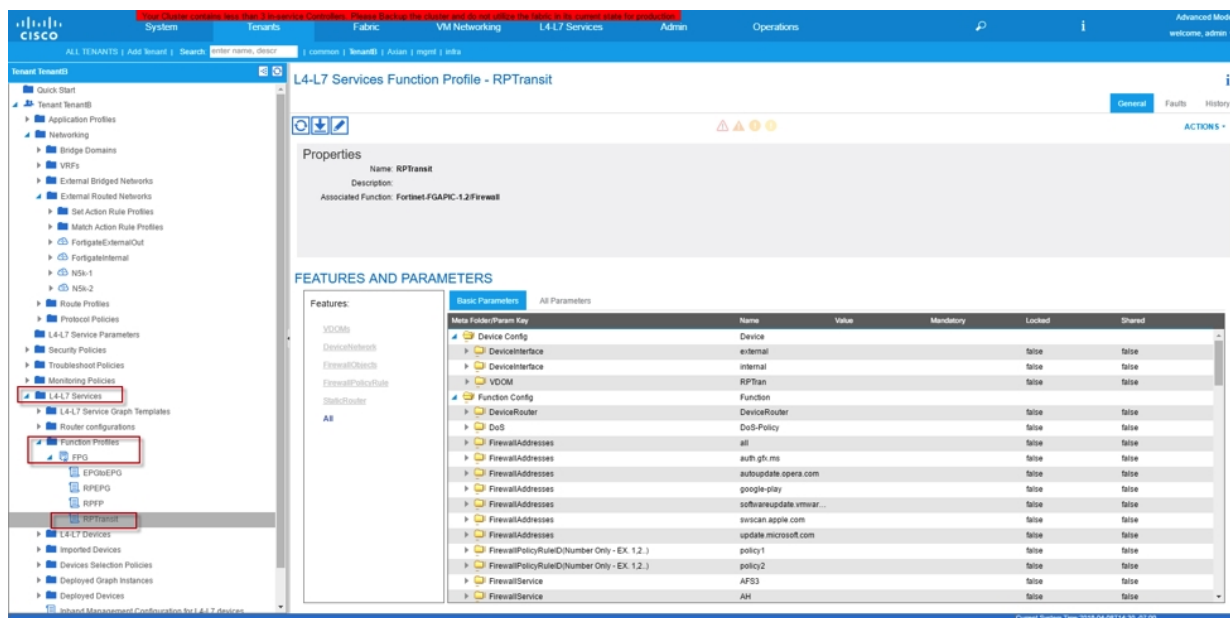
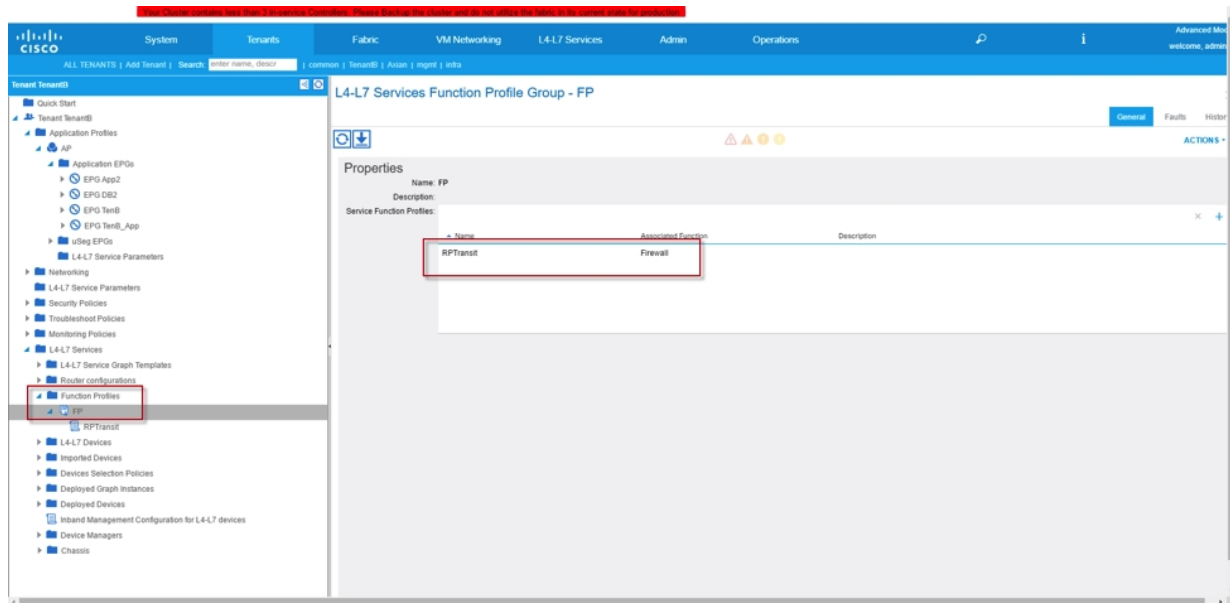




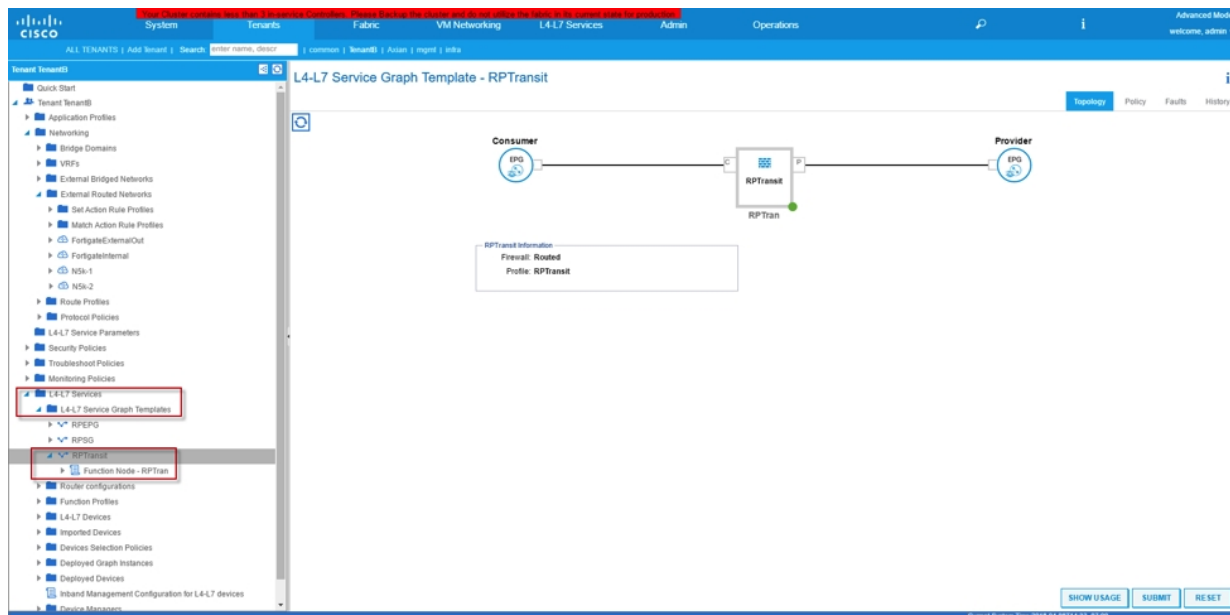
Configure Bridge Domain with Unicast Routing, assign SVI and associate L3Out to “FortigateInternal”



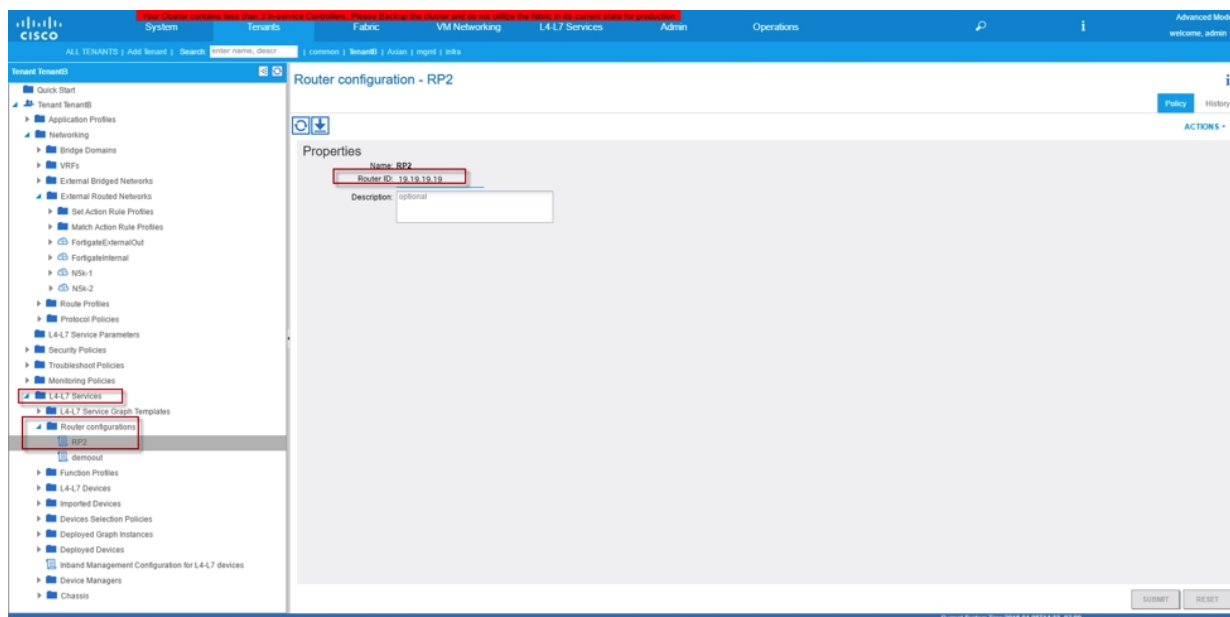
Create Functional Profile Group and Functional Profile from existing template



Create Service Graph template



Create Router ID that will be used on the Service Appliance (FortiGate)



Deploy Service Graph

L4-L7 Service Graph Template - RPTransit

Properties

Name: RPTransit
 Template Name: UNSPECIFIED
 Configuration Issues: optional
 Description: optional

Label:

Name	Function Name	Function Type	Description
RPTran	FortinetFGAPIC-12Firewall	GoTo	

Name	Provider/Consumer	Description
T1	Consumer	
T2	Provider	

Name	Connected Nodes	Unicast Route	Adjacency Type	Description
C1	RPTran, T1	True	L3	
C2	RPTran, T2	True	L3	

Buttons: SHOW USAGE, SUBMIT, RESET



Consumer will be App EPG. Provider is the DB EPG.

Apply L4-L7 Service Graph Template To EPGs

STEP 1 > Contract

1. Contract 2. Graph

Config A Contract Between EPGs

EPG Information

Consumer EPG / External Network: TenantB/AP/epg-App
 Provider EPG / External Network: TenantB/AP/epg-DB

Contract Information

Contract: Create A New Contract
 Contract Name: Contract
 No Filter (Allow All Traffic) ☒

Buttons: PREVIOUS, NEXT, CANCEL, SHOW USAGE, SUBMIT, RESET



Please select for Internal and external connections. In our example, we used “FortigateExternalOut” and FortigateInternal” as External and Internal selections respectively.

Apply L4-L7 Service Graph Template To EPGs

STEP 2 > Graph

1. Contract 2. Graph 3. RPTransit Parameters

Config A Service Graph

Device Clusters

- TenantB /EPGtoEPG (Managed Firewall)
- TenantB /FGRout (Managed Firewall)
- TenantB /RPEPG (Managed Firewall)
- TenantB /RPTransit (Managed Firewall)**

Graph Template: TenantB/RPTransit

Consumer: Fortigate_Out

Provider: Fortigate_In

RPTransit Information

Firewall: routed

Profile: RPTransit

Router Config: TenantB/RP2

Consumer Connector

Type: General **Route Peering**

L3 Ext Network: TenantB/FortigateExternalOut/Fortigate_Out

Cluster Interface: Ext

Provider Connector

Type: General **Route Peering**

L3 Ext Network: TenantB/FortigateInternal/Fortigate_In

Cluster Interface: Int

PREVIOUS NEXT CANCEL

Last minute check to make sure configuration is good before hit “Finish” button

Apply L4-L7 Service Graph Template To EPGs

STEP 3 > RPTransit Parameters

1. Contract 2. Graph 3. RPTransit Parameters

config parameters for the selected device

Profile Name: RPTransit <div id="vns-applyGraphTemplate2A:applyGraphNew3:applyProfile_editIcon" style="display: inline-block; width: 30px;"></div>

Features:

Required Parameters: **Add Parameters**

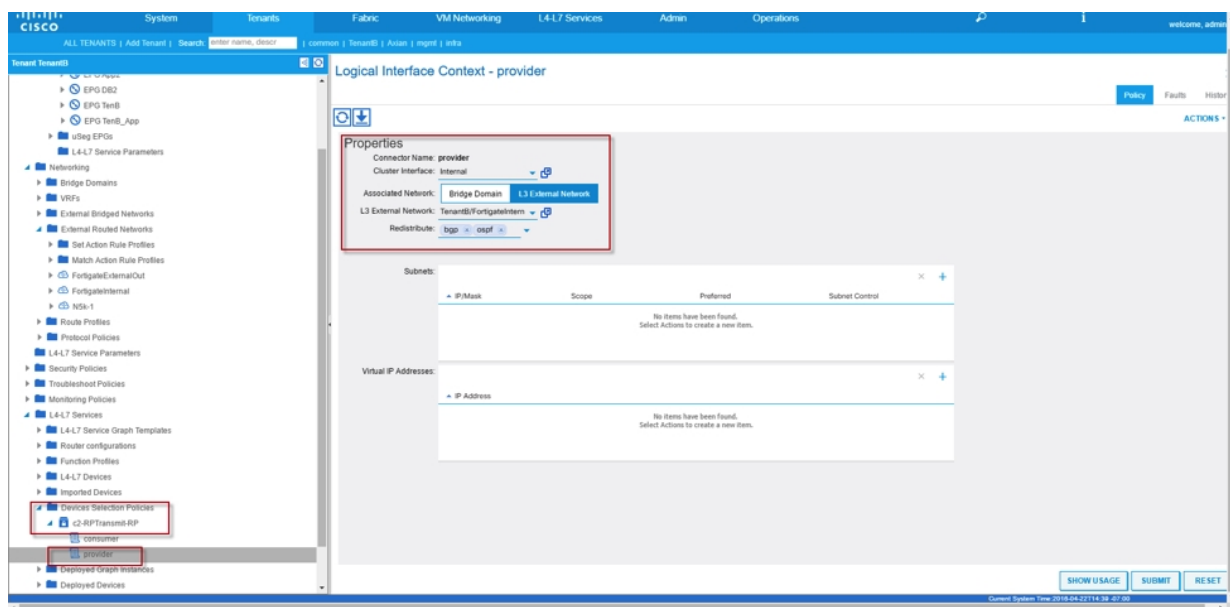
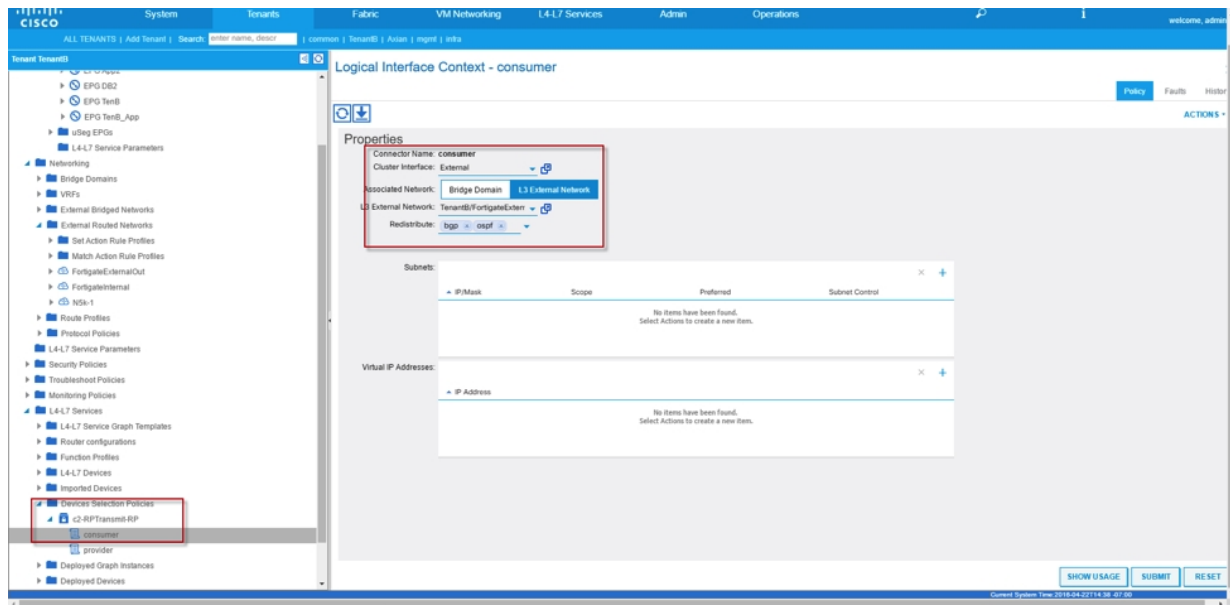
Folder/Param	Name	Value	Write Domain
Device Config	Device		
DeviceInterface	external		
DeviceInterface	internal		
VDOM	RPTran		
Function Config	Function		
DeviceRouter	DeviceRouter		
DoS	DoS-Policy		
FirewallAddresses	all		
FirewallAddresses	auth-g5.ms		
FirewallAddresses	adobeupdate.opera.com		
FirewallAddresses	google-play		
FirewallAddresses	softwareupdate.vmware.com		
FirewallAddresses	swscan.apple.com		
FirewallAddresses	update.microsoft.com		
FirewallAddresses	update.microsoft.com		

RED indicators parameters needed to be updated and GREEN indicates parameters will be submitted to the provider EPG.

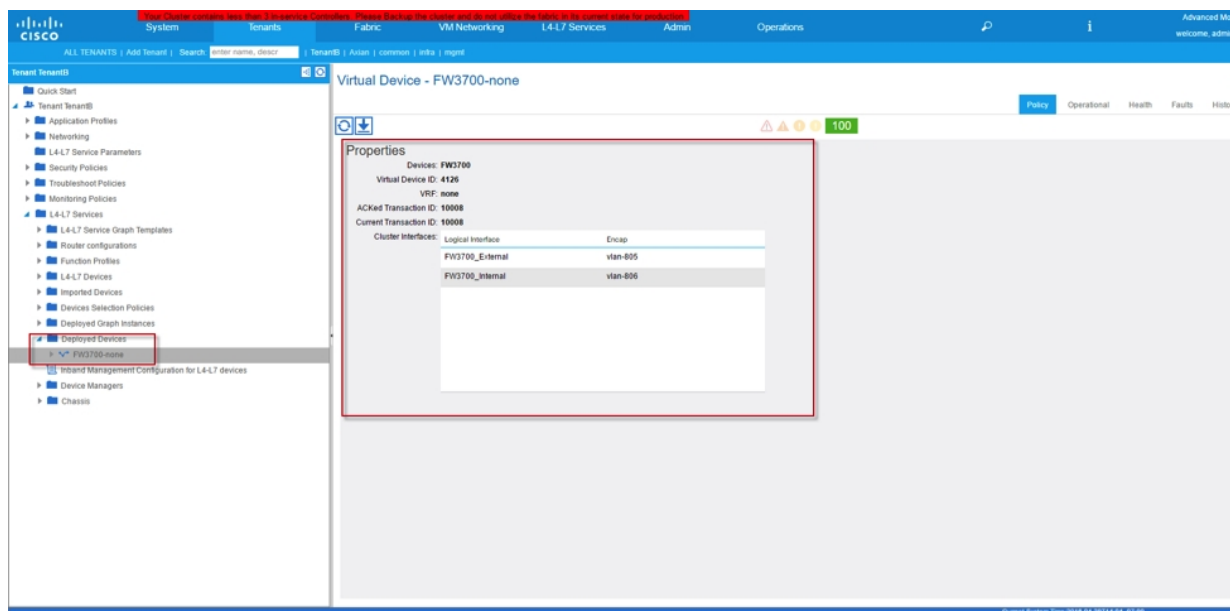
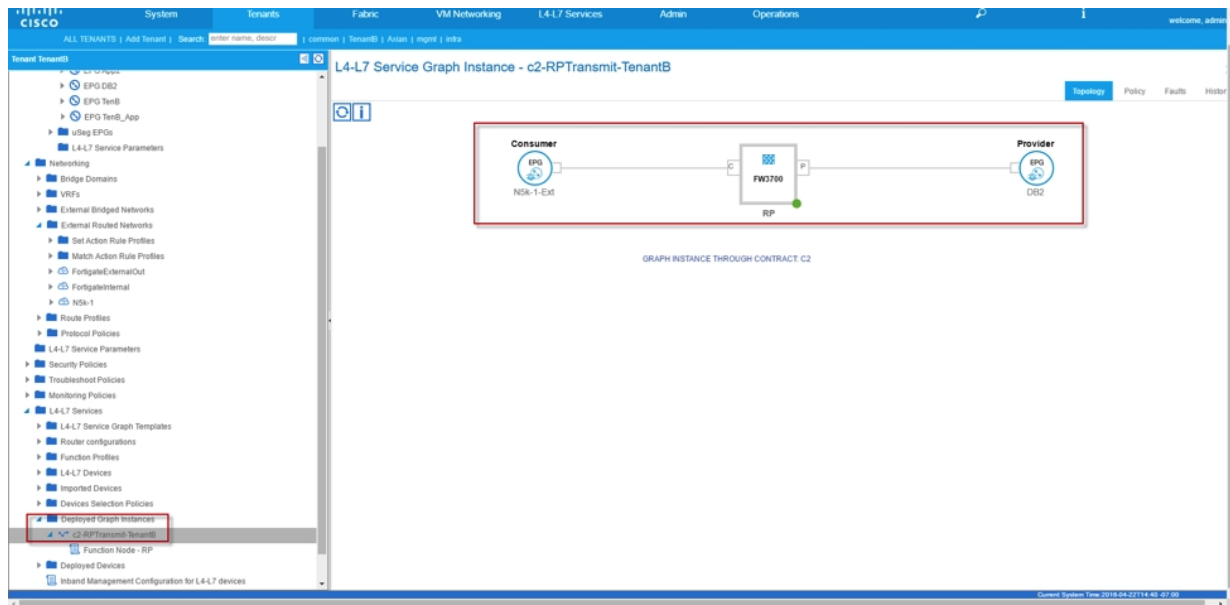
PREVIOUS **FINISH** CANCEL

SHOW USAGE SUBMIT RESET

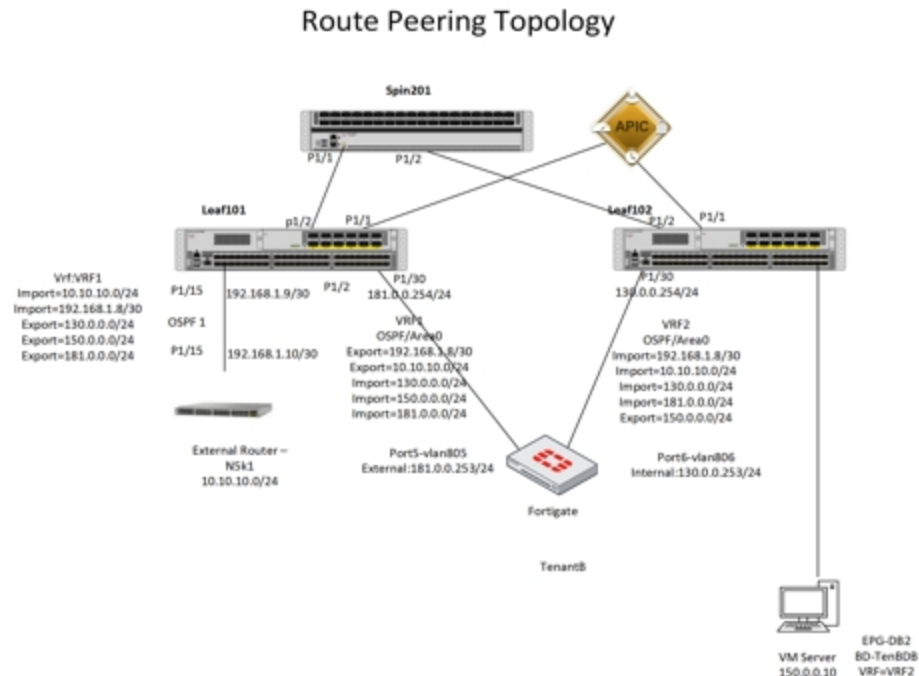
Check the status and verify Device Selection Policy



Verify deployed Graph Instance



Deploying Firewall Service for North-to-South traffic with OSPF



Introduction

This document describes the configuration walkthrough of L4-L7 Service Graph with Route Peering, where the consumer is external to ACI Fabric and the provider is internal to the Cisco ACI Fabric. With route peering feature provided by Cisco APIC, external traffic can reach internal servers through L4-L7 Services.

Prerequisites

Please pre-configure below configuration before deploying this design:

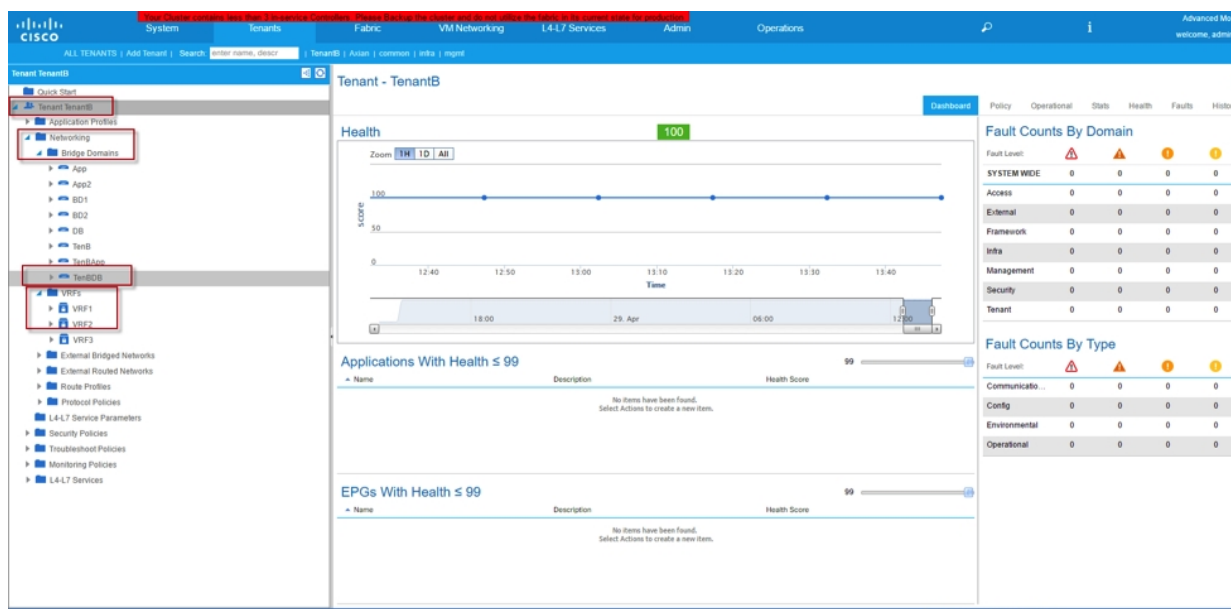
- Fabric Access Policies creation relating to:
 - VLAN Pools
 - Domain
 - Attachable Access Entity Profiles
 - Interface Policies
 - Switch Policies
- Layer3 Connection Outside of ACI Fabric
- L4-L7 Device Package has imported into Cisco APIC

Work Flow

1. Configure routing configuration on external router that attached to ACI Fabric
2. Create Tenant (TenantB in our example)
3. Create VRFs (VRF1 and VRF2 in our example)
4. Create Bridge Domain and map to VRF2 (TenBDB in our example)
5. Create EPG “EPG-DB2” and map it to Bridge Domain “TenBDB”
6. Create three L3Out EPGs (1 for external Connection, 1 for Firewall External and 1 for Firewall Internal. In our example, we used “N5k-1” for external Connection, “FortigateExternalOut” for Firewall External and “FortigateInternal” for Firewall Internal)
7. Create gateway IP on Bridge Domain (TenBDB) for VM Server
8. Ensure “Unicast Routing” is checked on Bridge Domain “TenBDB”
9. In Bridge Domain “TenBDB”, associate L3Outs to “FortigateInternal”
10. Map VM Server to EPG “EPG-DB2” and configure IP address and gateway ip address (TenBDB ip address)
11. Verify VM Server can ping to gateway IP
12. Create L4-L7 Device
13. Create Functional Profile Group as well as Functional Profile
14. Create Route Profiles
15. Create L4-L7 Service Graph Template
16. Deploy L4-L7 Service Graph

Configuration

Configure the Bridge Domain TenBDB, VRF1 and VRF2. Associate Bridge Domain TenBDB to VRF2



Configure L4-L7 Device for physical Fortigate (GoTo Mode)

L4-L7 Devices - RPTTransit

General

Managed: ☒ **Device 1**

Name: RPTTransit

Device Package: Fortinet-FGAPIC-1.2

Service Type: Firewall

Device Type: PHYSICAL

Physical Domain: FWDomain

Context Aware: Multiple

Function Type: GoThrough GoTo

Cluster Mode: Single Node

Credentials

Username: admin

Password:

Confirm Password:

Configuration State

Configuration Issues:

Devices State: stable

Device 1

Management IP Address: 10.160.11.13

Management Port: 443

Chassis: select a value

Interfaces

Name	Path
ports	Node-101eth1/30
ports	Node-102eth1/30

Cluster

Management IP Address: 10.160.11.13

Management Port: 443

Device Manager: select a value

Cluster Interfaces

Type	Name	Concrete Interfaces
consumer	Ext	RPTTransit_Device_1(port5)
provider	Int	RPTTransit_Device_1(port5)

Configure L3Out for N5K-1 and associate to VRF1



All L3Out Interfaces which are used for Route Peering are required to be configured as a SVI with Vlan Encapsulation accordingly.

L3 Outside - N5k-1

Properties

Tags:

Label:

Target DSCP: unspecified

Route Control Enforcement: ☐ Import ☒ Export

Resolved VRF: TenantB/VRF1

External Routed Domain: Internet

Route Profile for Interface: select a value

Route Control For Dampening

Address Family Type:

OSPF Area Control

Enable BGP/OSPF: ☐ BGP ☒ OSPF

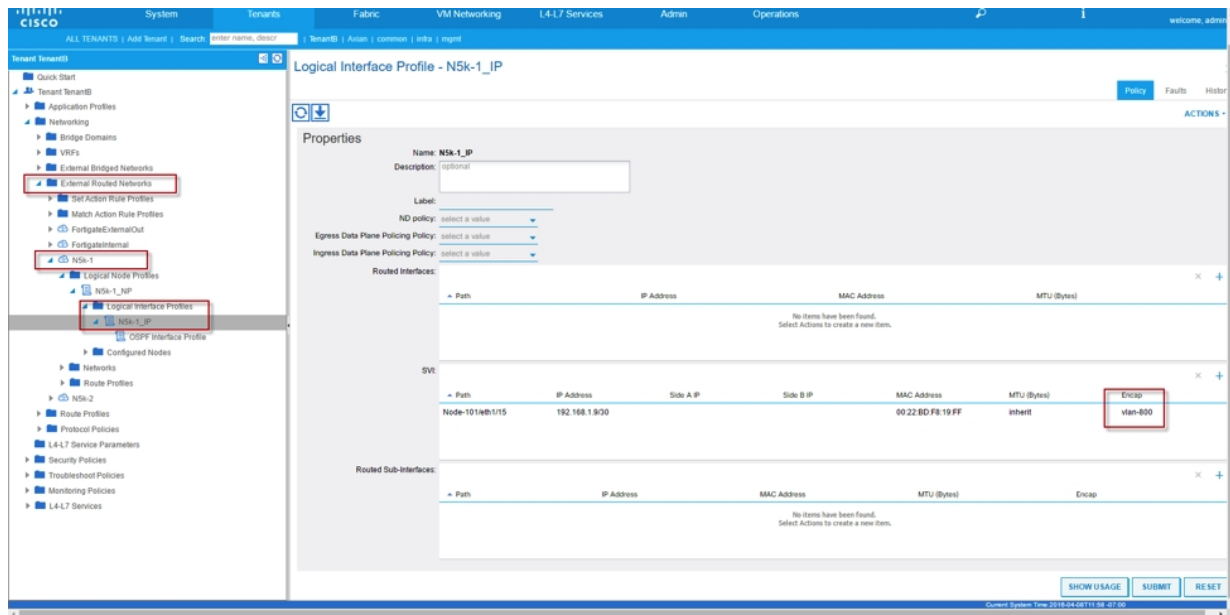
OSPF Area ID: 0.0.0.1

OSPF Area Control: ☒ Send redistributed LSAs into NSSA area ☒ Originate summary LSA ☐ Suppress forwarding address in translated LSA

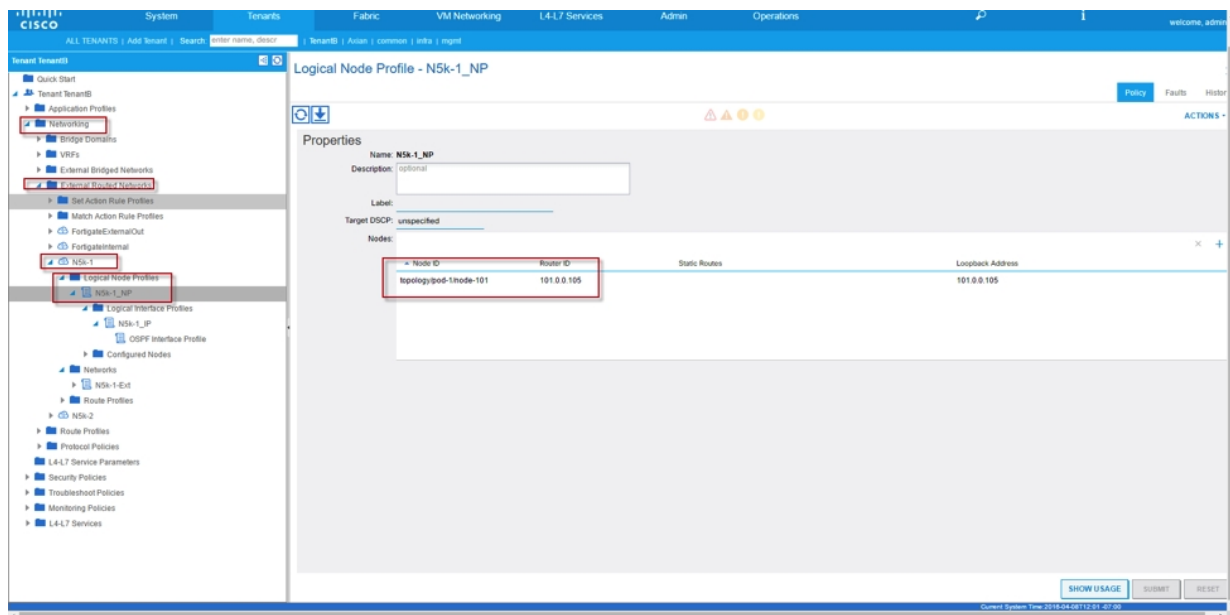
OSPF Area Type: NSSA area Regular area Stub area

OSPF Area Cost: 1

Configure SVI for L3Out N5k-1



Configure Route ID (101.0.0.105 in our example)



Configure Import/Export Route Control on Subnets for N5k-1 L3Out External EPG

External Network Instance Profile - N5k-1-Ext

Properties

Name: N5k-1-Ext

Tags: [empty]

Description: [optional]

Configured VRF name: VRF1

Resolved VRF: units-TenantB1c1c-VRF1

QoS Class: Unspecified

Target DSCP: unspecified

Configuration Status: **applied**

Configuration Issues:

Subnets	IP Address	Scope	Aggregate	Route Control Profile	Route Summarization Policy
	10.10.10.0/24	External Subnets for the External EPG			
	130.0.0.0/24	Export Route Control Subnet			
	150.0.0.0/24	Export Route Control Subnet			
	181.0.0.0/24	Export Route Control Subnet			
	192.168.1.0/30	External Subnets for the External EPG			

Route Control Profile: [empty]

No items have been found. Select Actions to create a new item.

Configure L3Out for Fortigate External Interface (FortigateExternalOut) and associate with VRF1



In our example, the route ID here must be the same as above (101.0.0.105), since both L3outs are on the same leaf switch.

L3 Outside - FortigateExternalOut

Properties

Tags: [empty]

Label: [empty]

Target DSCP: unspecified

Route Control Enforcement: ☒ Import ☒ Export

VRF: TenantB/VRF1

Resolved VRF: TenantB/VRF1

External Routed Domain: Internet

Route Profile for Interleaf: select a value

Route Control For Dampening:

Address Family Type: [empty]

Route Dampening Policy: [empty]

Enable BGP/EGRP/OSPF: ☐ BGP ☒ OSPF ☐ EIGRP

OSPF Area ID: 0

OSPF Area Control: ☒ Band redistributed LSAs into NSSA area ☒ Originate summary LSA ☐ Suppress forwarding address in translated LSA

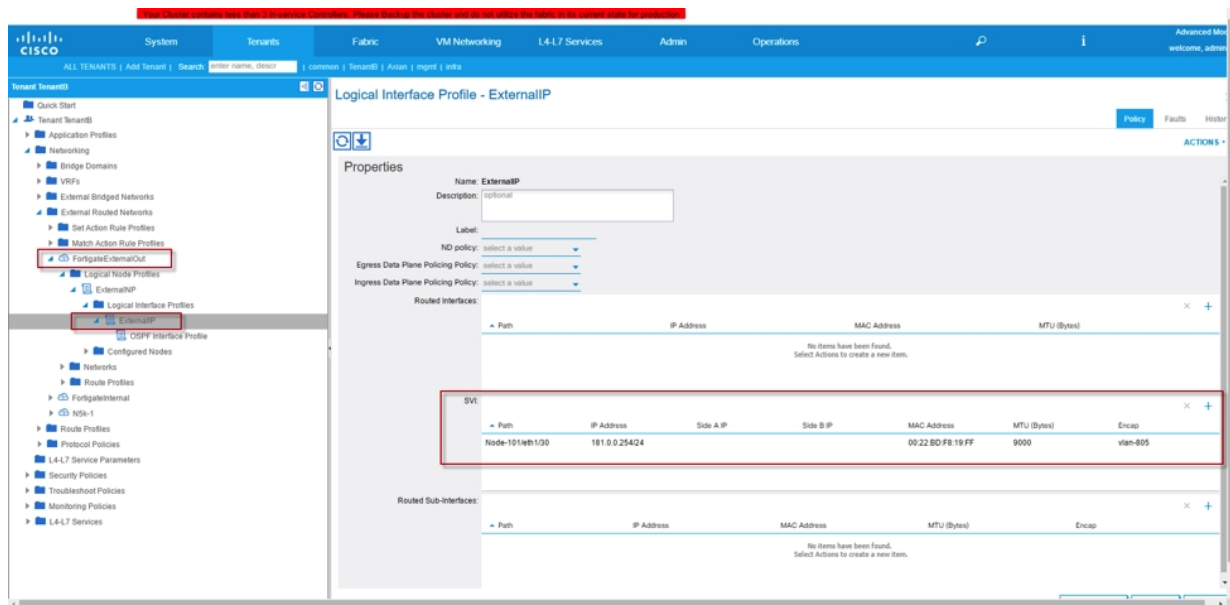
OSPF Area Type: NSSA area **Regular area** Stub area

OSPF Area Cost: 1

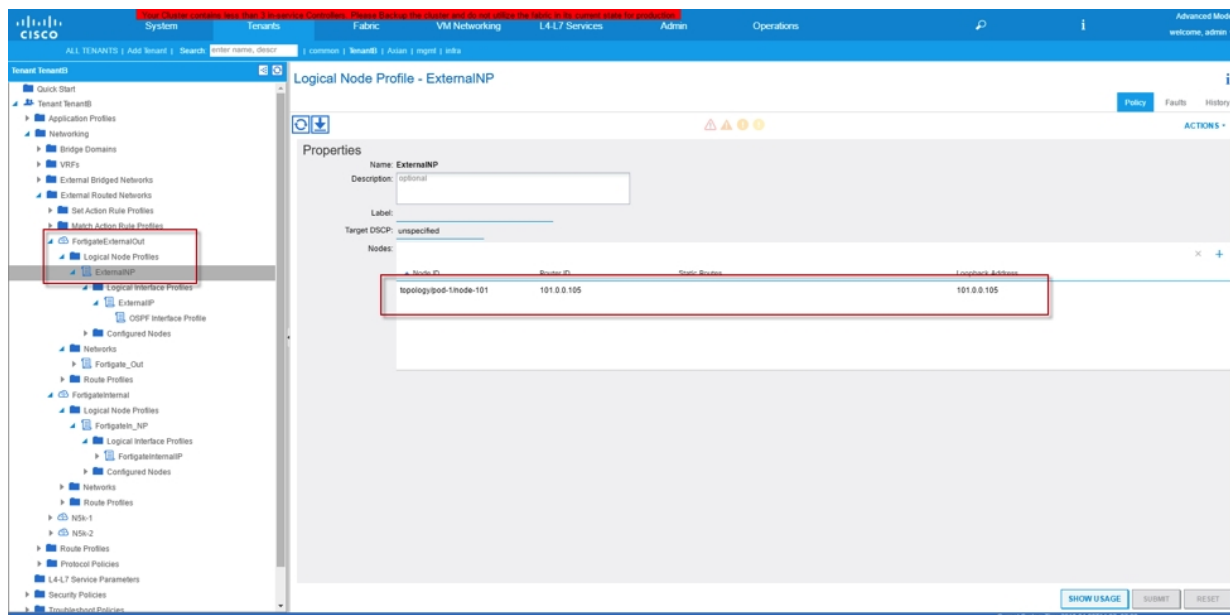
SHOW USAGE SUBMIT RESET

Current System Time: 2018-04-08T13:55:07:00

Configure SVI for L3Out Fortigate External out (FortigateExternalOut)



Configure Route ID for L3Out Fortigate External Out (FortigateExternalOut)



Configure Import/Export Route Control on Subnets for Fortigate External out

External Network Instance Profile - Fortigate_Out

Properties

Name: Fortigate_Out

Tags:

Description:

Configured VRF name: VRF1

Resolved VRF: units-TenantB1ctx-VRF1

QoS Class: Unspecified

Target DSCP: unspecified

Configuration Status: applied

Configuration Issues

Subnets	Scope	Aggregate	Route Control Profile	Route Summarization Policy
10.10.0.0/24	Export Route Control Subnet			
130.0.0.0/24	External Subnets for the External EPG			
150.0.0.0/24	External Subnets for the External EPG			
181.0.0.0/24	External Subnets for the External EPG			
192.168.1.0/24	Export Route Control Subnet			

Configure L3Out for Fortigate Internal (FortigateInternal) and associate with VRF2

L3 Outside - FortigateInternal

Properties

Tags:

Label:

Target DSCP: unspecified

Route Control Enforcement: ☒ Import ☐ Export

VRF: TenantB/VRF 2

Resolved VRF: TenantB/VRF2

External Routed Domain: Internet

Route Profile for Interleaf: select a value

Route Control For Dampening:

Enable BGP/EGRP/OSPF: ☐ BGP ☐ EGRP ☒ OSPF

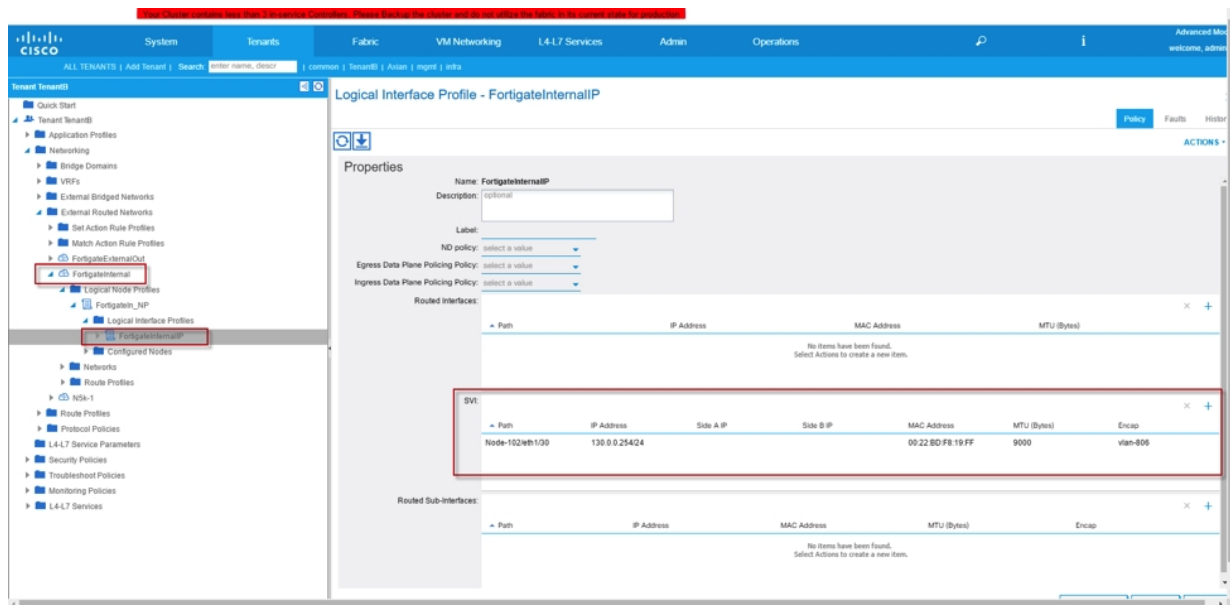
OSPF Area ID: 0

OSPF Area Control: ☒ Send redistributed LSAs into NSSA area ☒ Originate summary LSA ☐ Suppress forwarding address in translated LSA

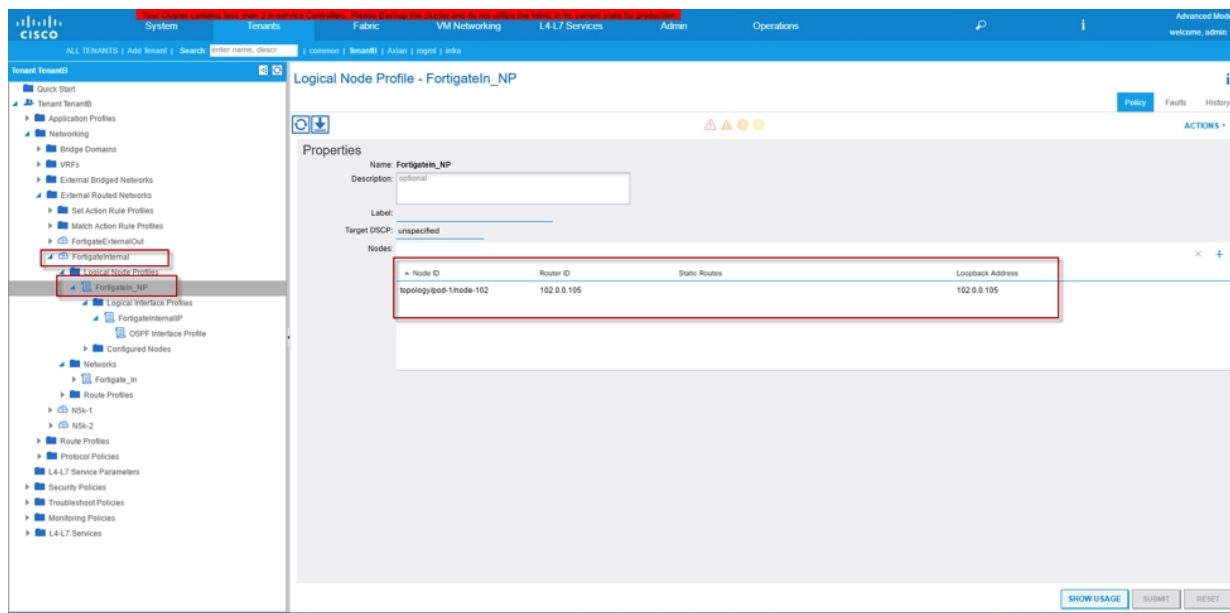
OSPF Area Type: ☒ NSSA area ☐ Regular area ☐ Stub area

OSPF Area Cost: 1

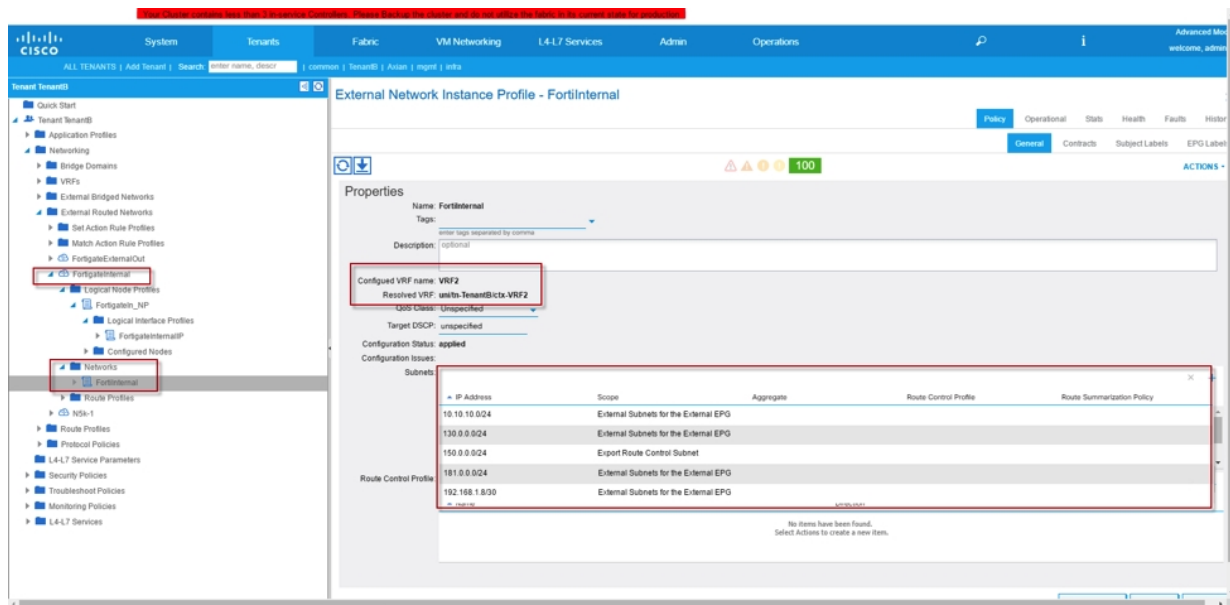
Configure SVI for L3Out Fortigate Internal (FortigateInternal)



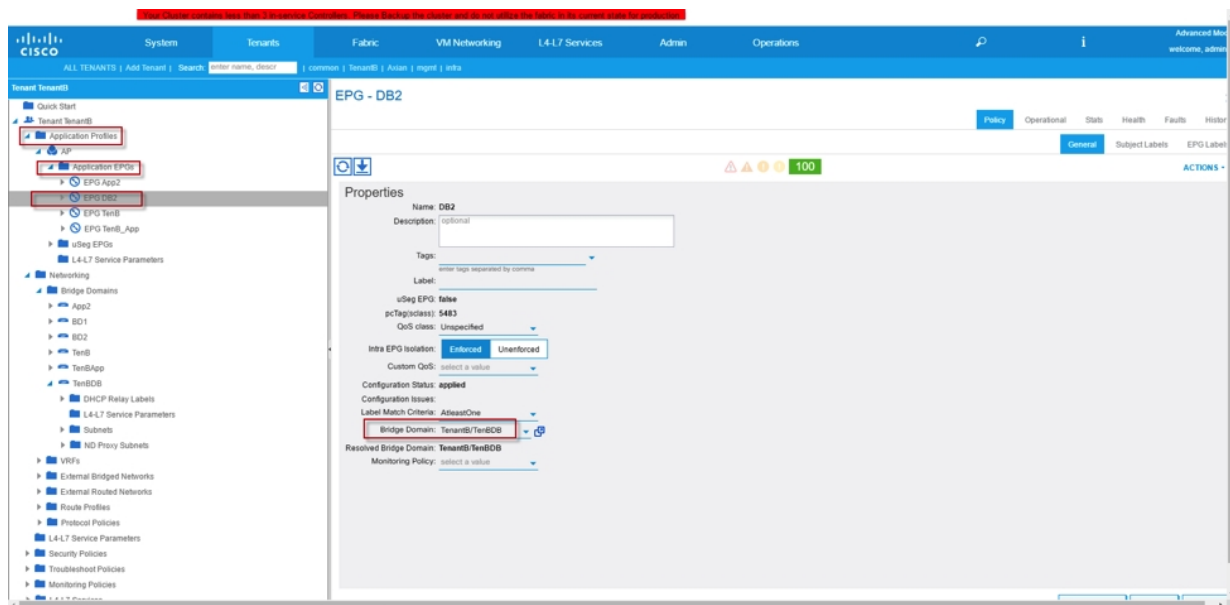
Configure Route ID for L3Out Fortigate Internal (FortigateInternal)

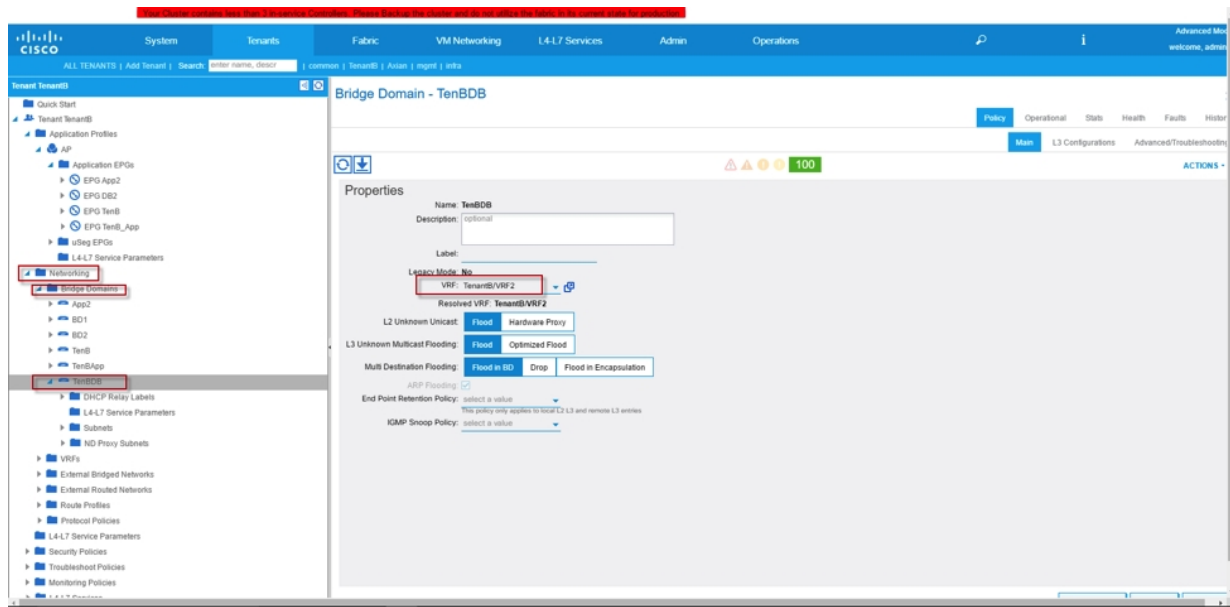


Configure Import/Export Route Control on Subnet for L3Out Fortigate Internal (FortigateInternal)

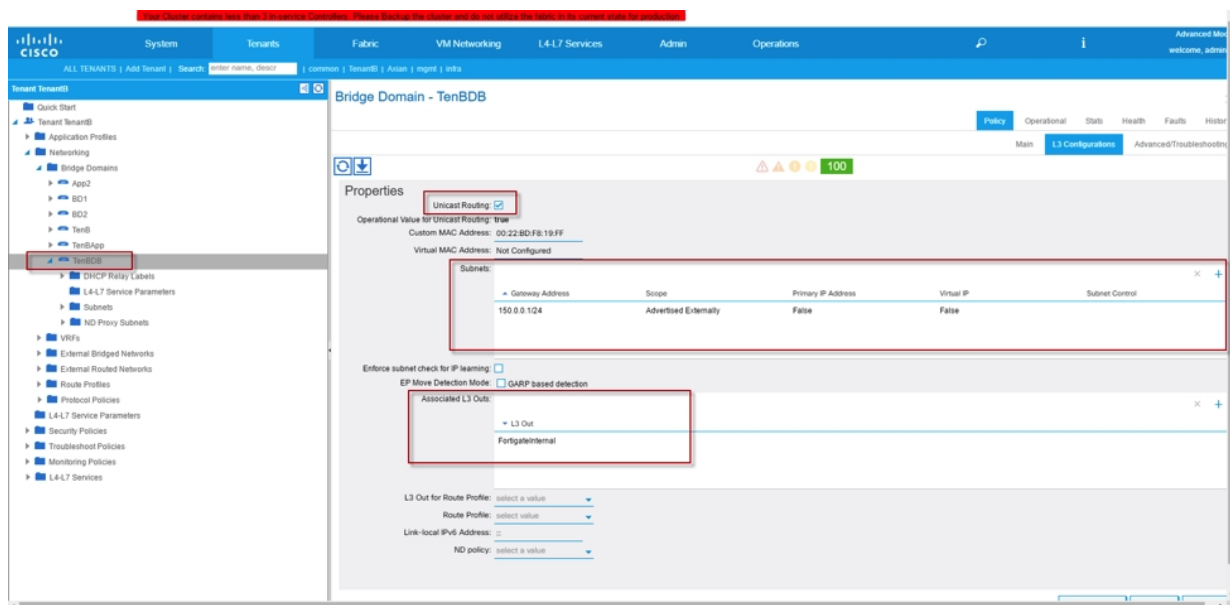


Associate EPG "DB2" to Bridge Domain "TenBDB" and attach Bridge Domain to VRF2

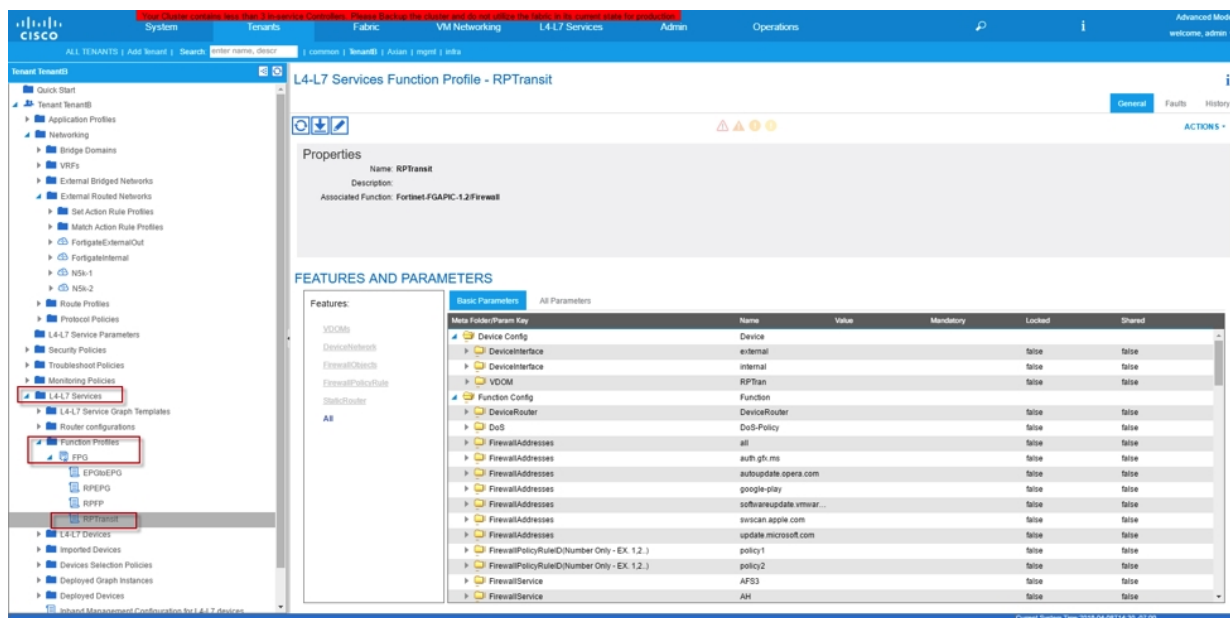
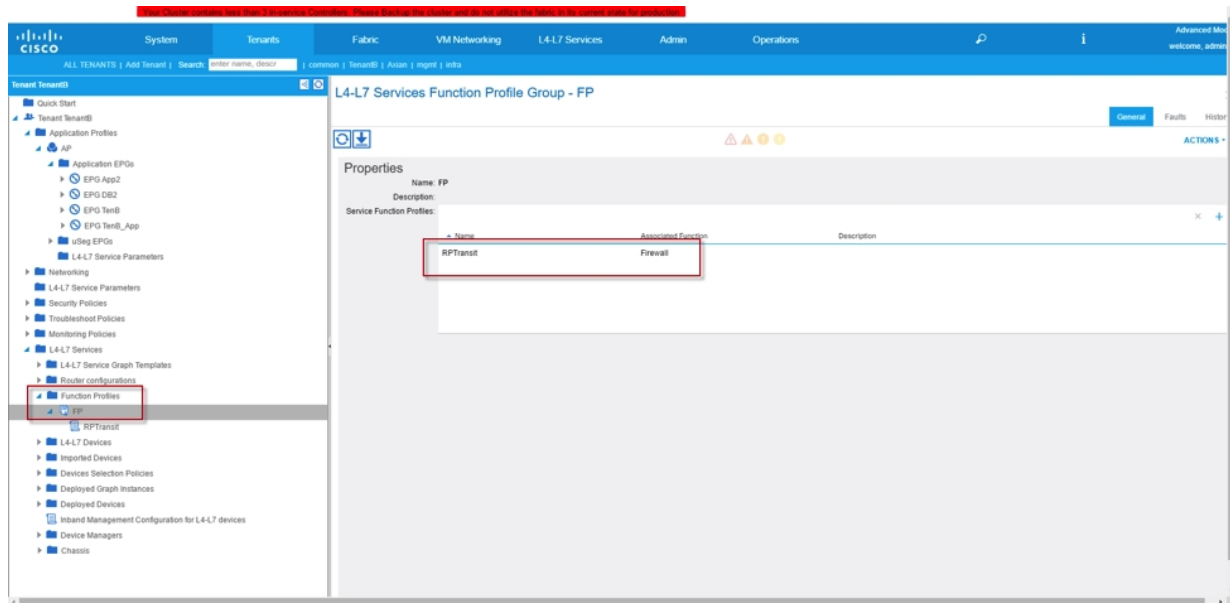




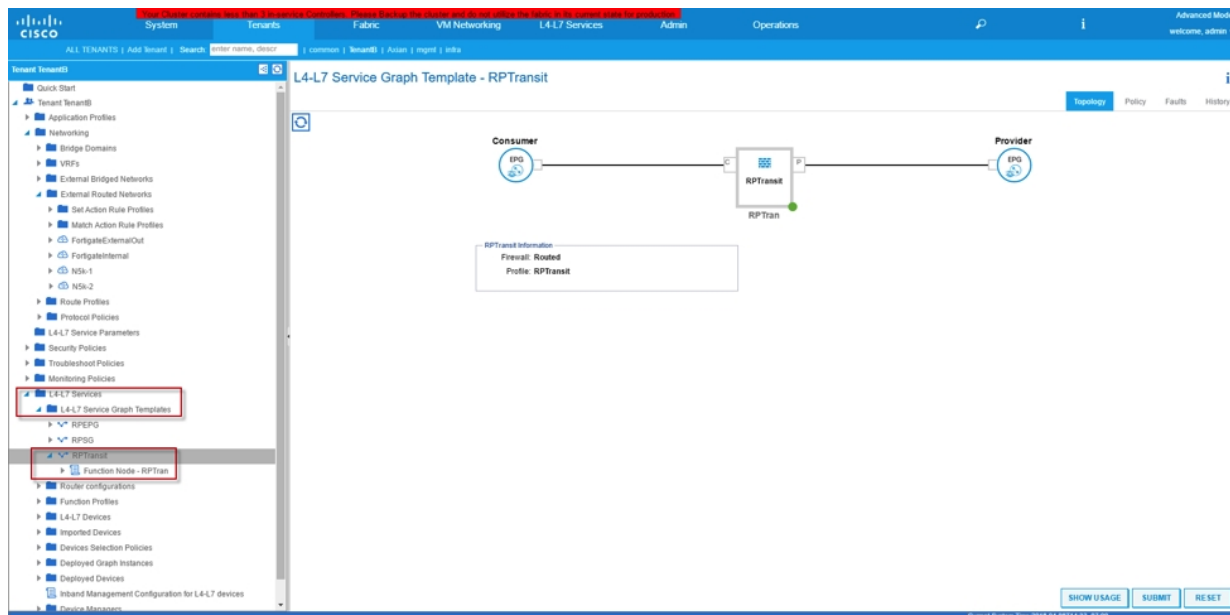
Configure Bridge Domain with Unicast Routing, assign SVI and associate L3Outs to “FortigateInternal”



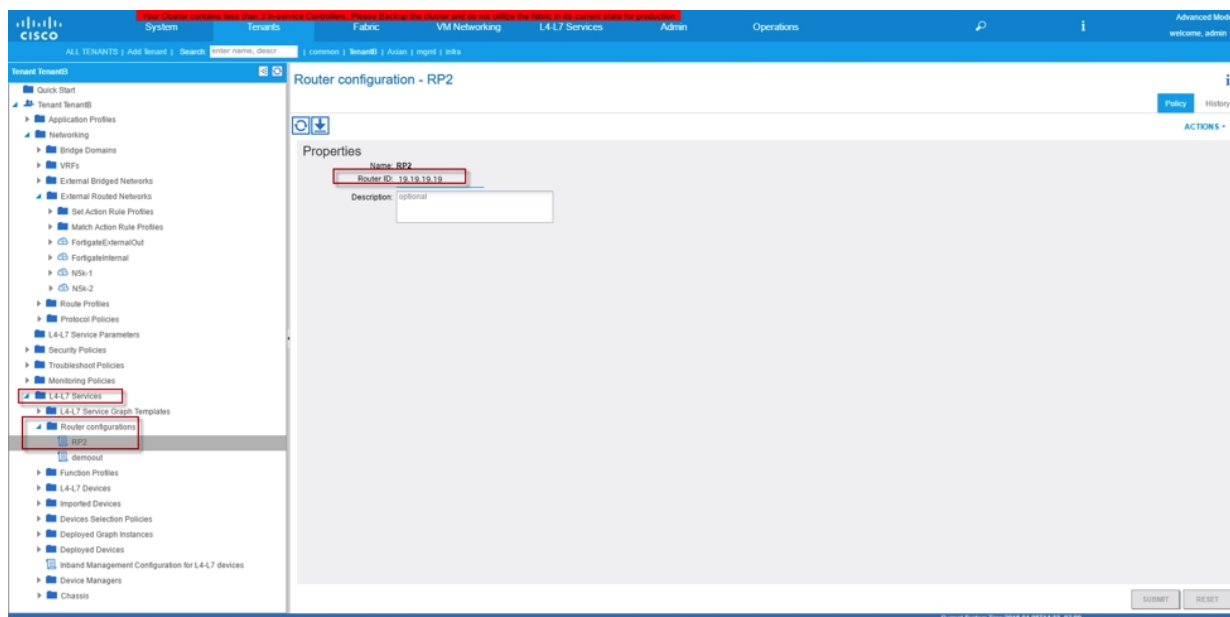
Create Functional Profile Group and Functional Profile from existing template



Create Service Graph template



Create Router ID that will be used on the Service Appliance (Fortigate)



Deploy Service Graph



Consumer will be L3Outs facing external router. Provider is the internal EPG. In our case will be N5k-1 and DB2 respectively.



Route peering needs to be select for Internal and external connections. In our example, we used "FortigateExternalOut" and FortigateInternal" as External and Internal selections respectively.

Apply L4-L7 Service Graph Template To EPGs

STEP 2 > Graph

1. Contract 2. Graph 3. RPTransit Parameters

Config A Service Graph

Device Clusters

- TenantB /EPGtoEPG (Managed Firewall)
- TenantB /FGRtoRoute (Managed Firewall)
- TenantB /RPtoEPG (Managed Firewall)
- TenantB /RPTransit (Managed Firewall)**

Graph Template: TenantB/RPTransit

Consumer: Fortigate_Out

Provider: Fortigate_In

RPTransit Information

Firewall: routed

Profile: RPTransit

Router Config: TenantB/RP2

Consumer Connector

Type: General **Route Peering**

L3 Ext Network: TenantB/FortigateExternalOut/Fortigate_Out

Cluster Interface: Ext

Provider Connector

Type: General **Route Peering**

L3 Ext Network: TenantB/FortigateInternal/Fortigate_In

Cluster Interface: Int

PREVIOUS NEXT CANCEL

Last minute check to make sure configuration is good before hit “Finish” button

Apply L4-L7 Service Graph Template To EPGs

STEP 3 > RPTransit Parameters

1. Contract 2. Graph 3. RPTransit Parameters

config parameters for the selected device

Profile Name: RPTransit <div id="vns:applyGraphTemplate2A:applyGraphNew3:applyProfile_editIcon" style="display: inline-block; width: 30px;"></div>

Required Parameters: **All Parameters**

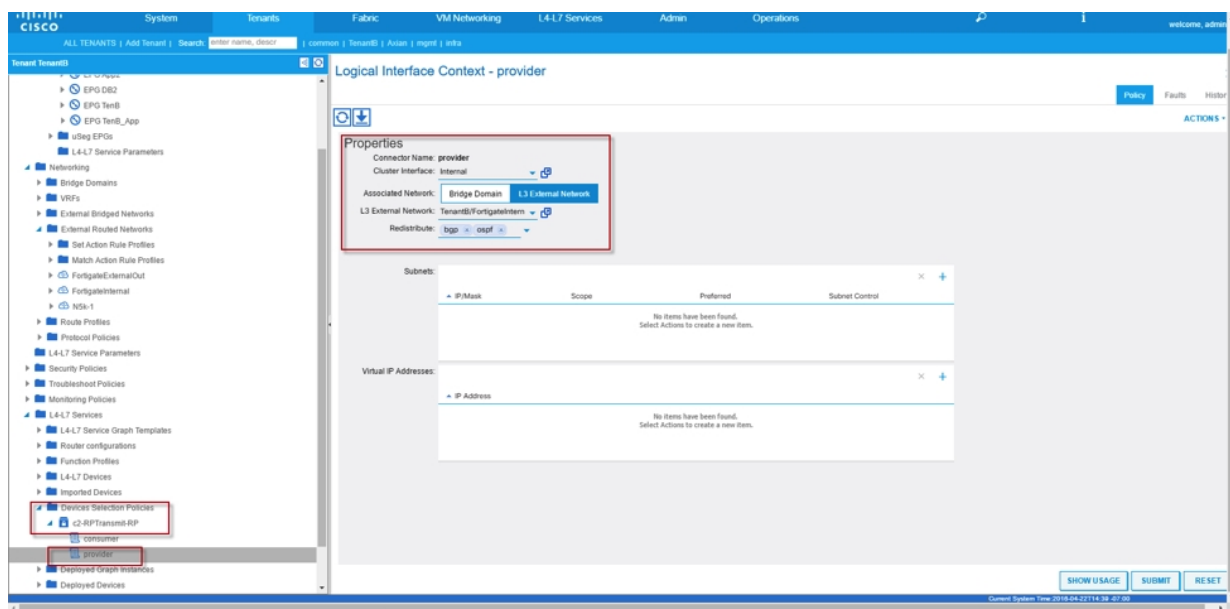
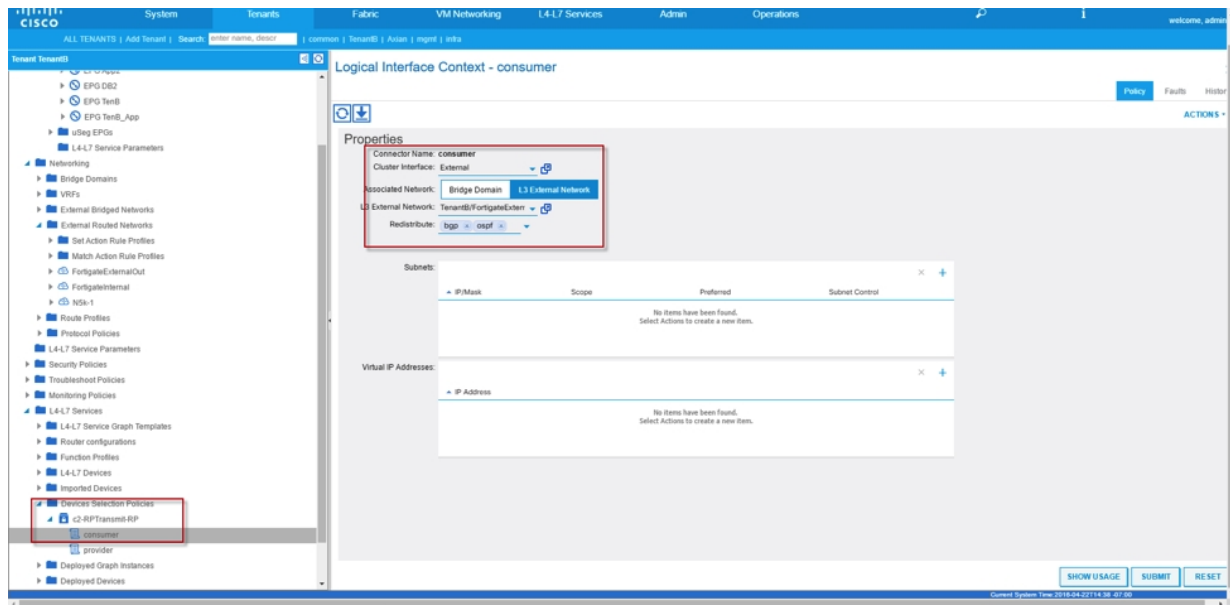
Feature	Folder/Param	Name	Value	Write Domain
VDOMs	Device Config	Device		
	DeviceInterface	external		
FirewallObjects	DeviceInterface	internal		
	VDOM	RPTran		
FirewallPolicyRule	Function Config	Function		
	DeviceRouter	DeviceRouter		
StaticRouter	DoS	DoS-Policy		
	FirewallAddresses	all		
AT	FirewallAddresses	auth-gn.ms		
	FirewallAddresses	autoupdate.opera.com		
	FirewallAddresses	google-play		
	FirewallAddresses	softwareupdate.vmware.com		
	FirewallAddresses	services.apple.com		
	FirewallAddresses	update.microsoft.com		

RED indicators parameters needed to be updated and GREEN indicates parameters will be submitted to the provider EPG.

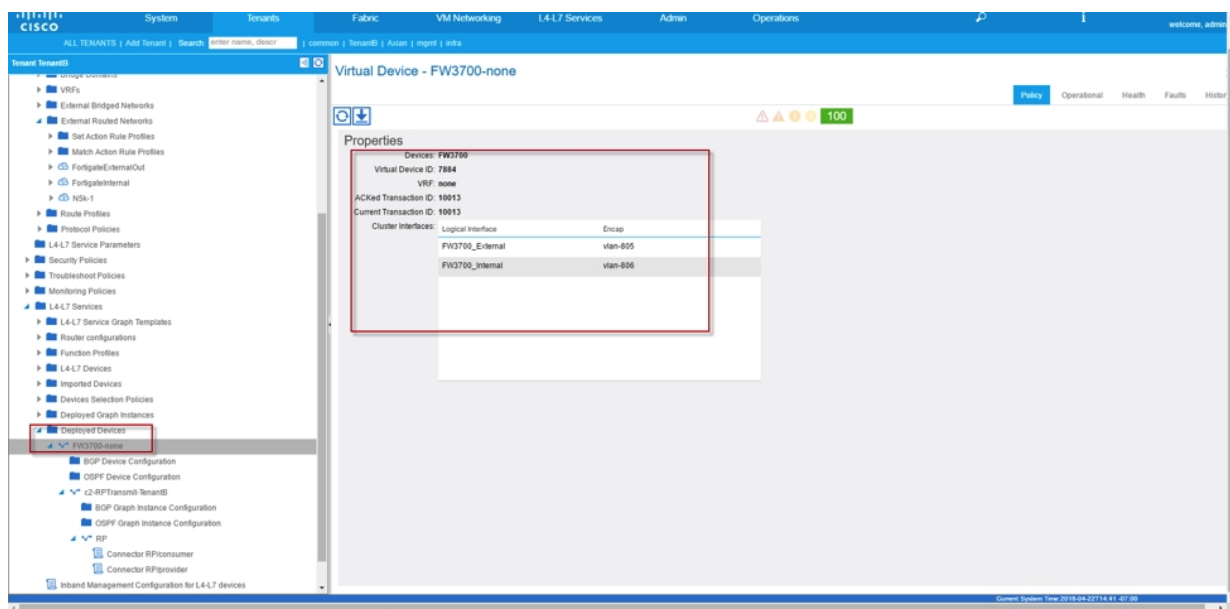
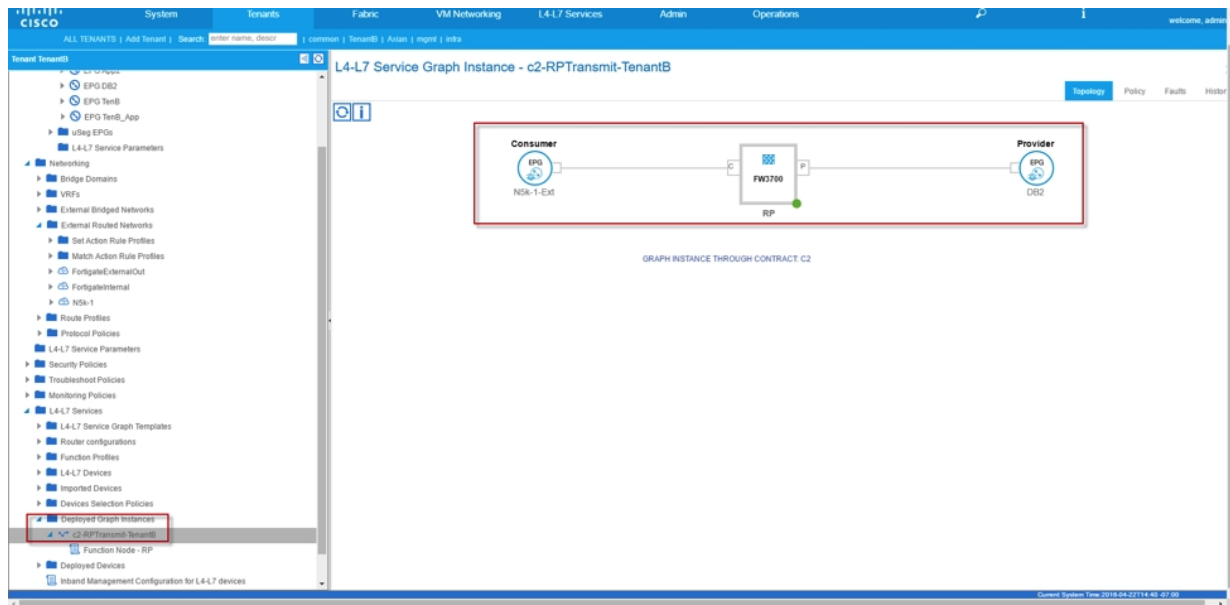
PREVIOUS **FINISH** CANCEL

SHOW USAGE SUBMIT RESET

Check the status and verify Device Selection Policy



Verify deployed Graph Instance



Deploying High Availability Service with Cisco ACI and FortiGate

Pre-requisite

On Fortigate

- Configure Fortigate HA Pair (Active-Standby Mode). Please consult Fortinet support website for setting up HA procedures.

On APIC

- Fabric Access Policies creation relating to:
 - VLAN Pools
 - Domain
 - Attachable Access Entity Profiles
 - Interface Policies
 - Switch Policies
- Create Tenant, VRF, 2 Bridge Domains, 2 EPGs
- Associate 2 Bridge Domains to VRF
- Associate 2 EPGs to the 2 Bridge Domains
- L4-L7 Device Package has imported into Cisco APIC

Work Flow

1. Create Go-Through Mode with HA enabled, then configure Device #1 and Device #2 on Cisco APIC
2. Create Functional Profile
3. Create Service Graph Template
4. Deploy Service Graph

In general, the procedures to deploy a Go-Through mode HA scenario vs regular Go-Through mode deployment are identical with the exception of enabling HA during L4-L7 device configuration. User needs to select HA Cluster instead of Single Node for Mode selection; there will be two devices appear on the screen where user will input the same Active Fortigate IP address and the corresponding connection ports between Fortigates and Cisco APIC for both devices. Please see below screen shot for reference.

L4-L7 Devices - FG3700

[Policy](#)[Parameters](#)[Faults](#)[History](#)

[ACTIONS](#)

General

Managed: ☒

Name: FG3700

Device Package: Fortinet-FGAPIC-1.3

Service Type: Firewall

Device Type: PHYSICAL

Physical Domain: FWDomain

Context Aware: Multiple

Function Type: GoThrough

Credentials

Username: admin

Password:

Confirm Password:

Configuration State

Configuration Issues:

Devices State: stable

Devices

Name	Management Address	Management Port	Interfaces
Device1	10.160.11.13	443	PO1 (Pod-1/Node-101-102/VPC1_Active)
Device2	10.160.11.13	443	PO1 (Pod-1/Node-101-102/VPC2_3719Standby)

Cluster

Management IP Address: 10.160.11.13 Management Port: 443

Device Manager: select a value

Cluster Interfaces:

Type	Name	Concrete Interfaces
consumer	external	Device1/[PO1], Device2/[PO1]
provider	internal	Device1/[PO1], Device2/[PO1]

Deploying Firewall service with Fortigate-VM and VMware

Pre-requisite

- Fabric Access Policies creation relating to:
 - VLAN Pools
 - Domain
 - Attachable Access Entity Profiles
 - Interface Policies
 - Switch Policies
- Create Tenant, VRF, 2 Bridge Domains, 2 EPGs
- Associate 2 Bridge Domains to VRF
- Associate 2 EPGs to the 2 Bridge Domains
- Layer4-7 Device Package has imported into Cisco APIC

Work Flow

1. Create Go-Through mode Fortigate VM Devices on Cisco APIC
2. Create Functional Profile
3. Create Service Graph Template
4. Deploy Service Graph

Configuration

Create Layer 4-L7 Device on Cisco APIC

The screenshot displays the Cisco APIC GUI for configuring L4-L7 Devices. The left sidebar shows the navigation tree with 'L4-L7 Devices' selected. The main panel is titled 'L4-L7 Devices - FGVM12' and contains the following configuration details:

- General:**
 - Managed: ☒
 - Name: FGVM12
 - Device Package: Fortinet-FGAPIC-1.2
 - Service Type: Firewall
 - Device Type: VIRTUAL
 - VMM Domain: vcenter
 - Content Aware: Single
 - Function Type: GoThrough
 - Cluster Mode: Single Node
- Credentials:**
 - Username: admin
 - Password: (masked)
 - Confirm Password: (masked)
- Configuration State:**
 - Configuration Issues: (empty)
 - Device State: stable
- Device 1:**
 - Management IP Address: 10.160.11.103
 - Management Port: 443
 - vCenter Name: vcenter
 - VM Name: FGVM103
 - Chassis: select a value
- Interfaces:**

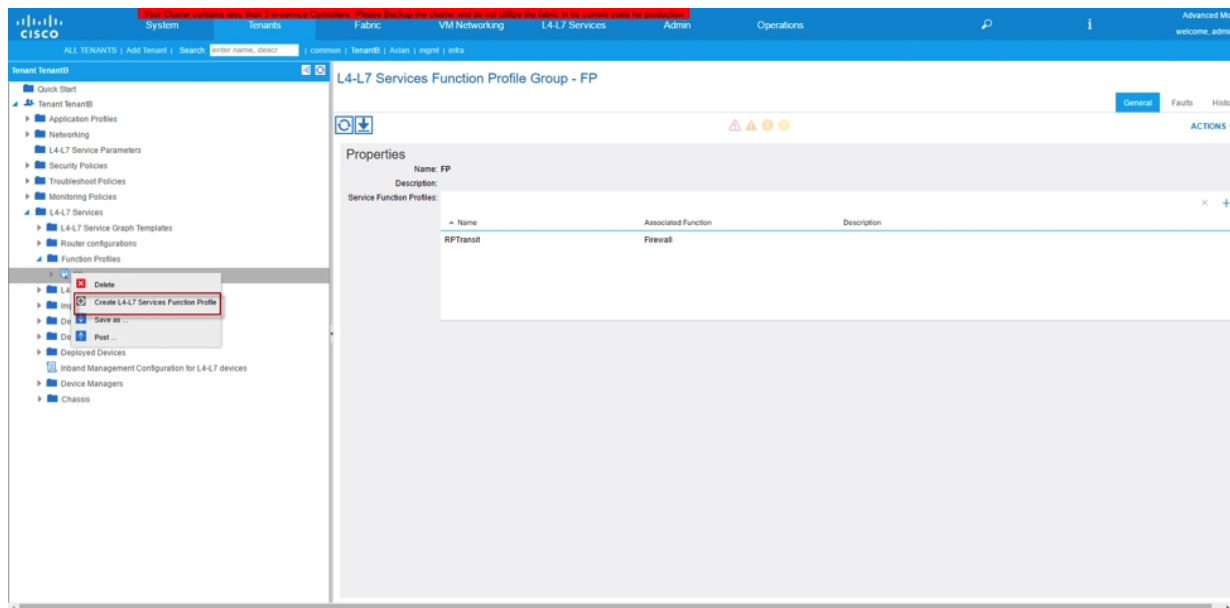
Name	VNIC	Path (Only For Route Peering)
port2	Network adapter 2	Node-101neth102
port3	Network adapter 3	Node-101fex-101neth102
- Cluster:**
 - Management IP Address: 10.160.11.103
 - Management Port: 443
 - Device Manager: select a value
- Cluster Interfaces:**

Type	Name	Concrete Interfaces
provider	ins	FGVM12_Device_1[port2]
consumer	out	FGVM12_Device_1[port3]

At the bottom right, there are buttons for 'SHOW USAGE', 'SUBMIT', and 'RESET'.

Create Functional Profile

Functional Profile defines the template for the Service(s) that is going to deploy such as L4-L7 Device Interface IP addresses, Rule ID, Object Addresses, Policy Rules, Source/Destination Ports...etc.



Functional Profile Objects Explanation

Device Config

Contained External and Internal Interfaces that will be programmed onto Fortigate VDOM. This is the interfaces (typically external and internal) that will be associated to the VDOM.



Similar to above notes, for Go-To Mode, please modify the IP address field otherwise leave the default for Go-Through Mode.

Function Config

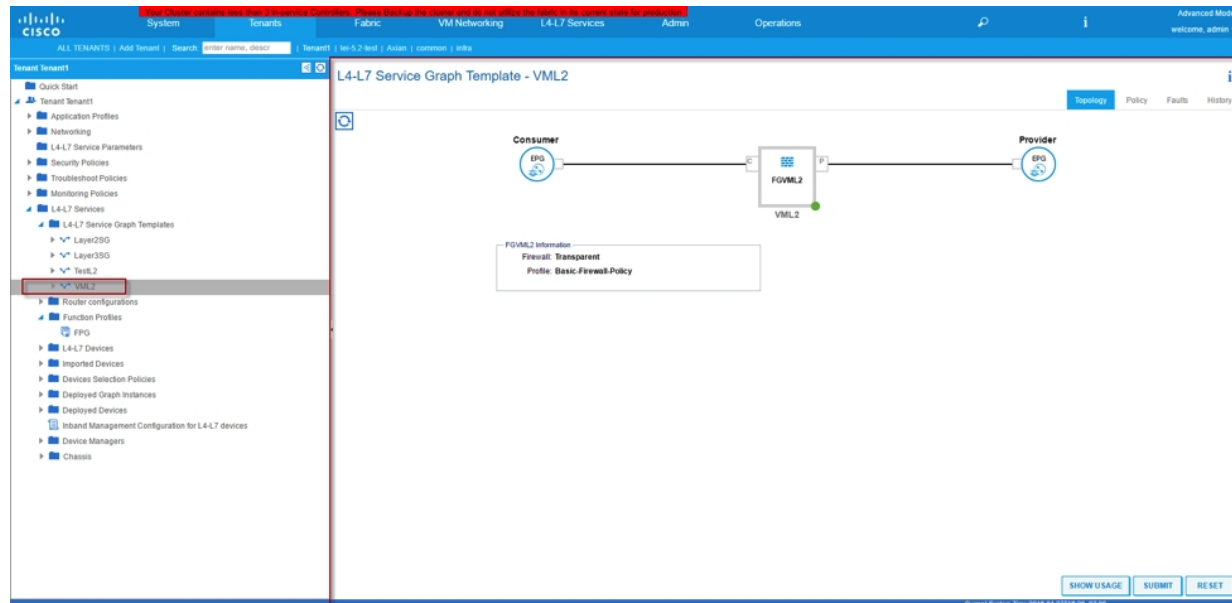
Function Config consist of:

- **Network**
 - This field is use for configure Static Routes for IPv4 and IPv6.
- **Policy and Objects**
 - This folder is the container for following list of Folders:
 - a. FWServiceFolder – Firewall Service Object container
 - b. IPv4/IPv6 DoS Policy – Dos Policy configuration
 - c. IPv4/IPv6 FirewallAddresses – Firewall Addresses Object container
 - d. IPv4 Policy – Firewall Policy Rule container

- e. IPv4 FirewallAddresses Group – Group folder for “Dynamic EPG” feature
- f. ScheduleFolder – Schedule container
- **VDOM-Folder**
 - VDOM internal and external interfaces

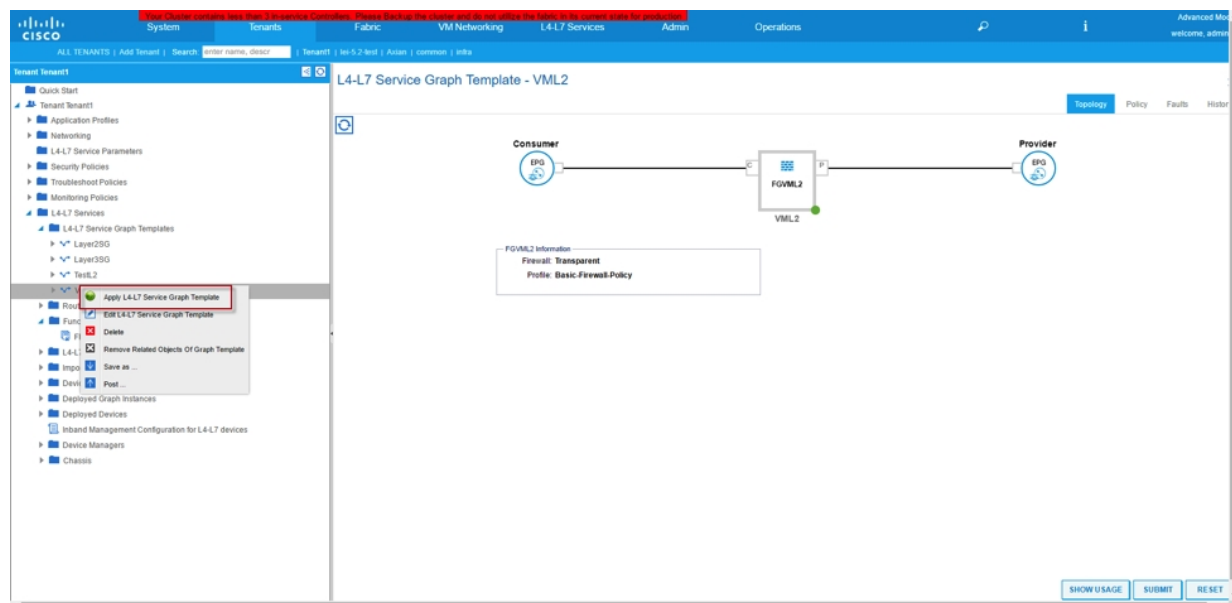
Create Service Graph

Service Graph template is used to tightly coupled the Functional Profile or Firewall configuration and combine with the Firewall device we defined at earlier steps.

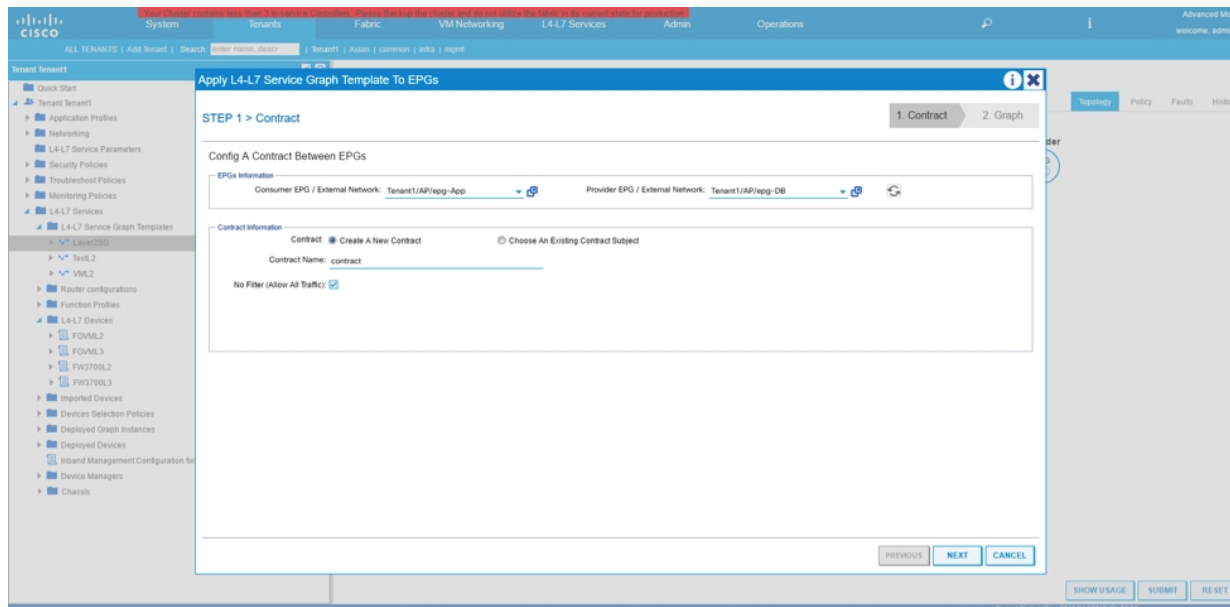


Deploy Service Graph

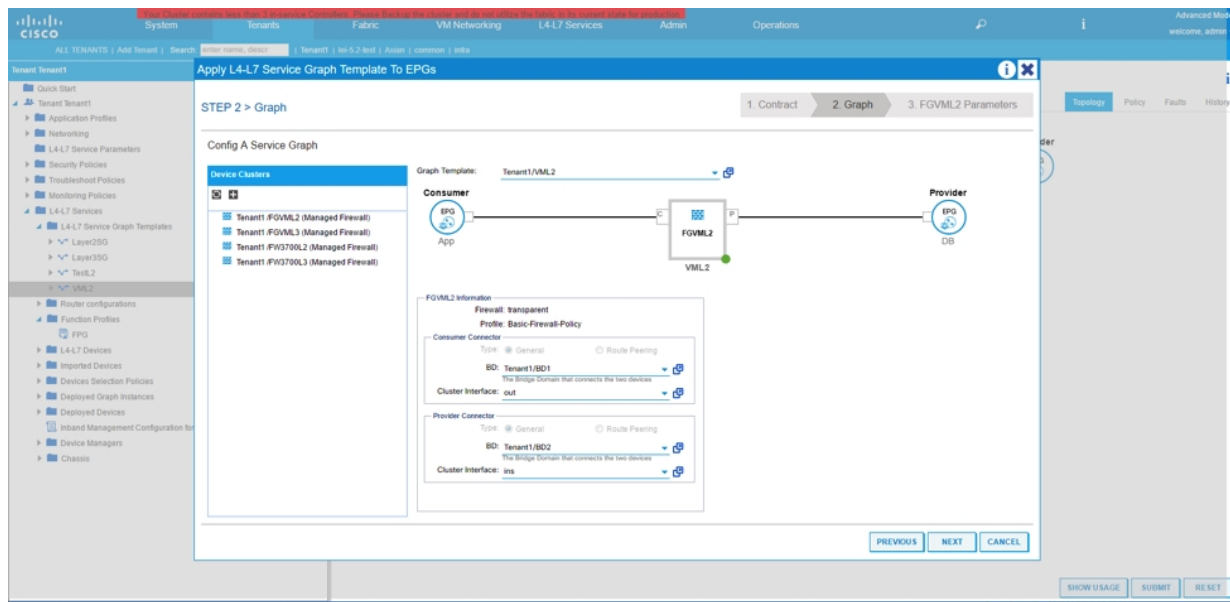
Once we combined the Firewall configuration and associated device together, we are ready to deploy the service Graph to create a VDOM.



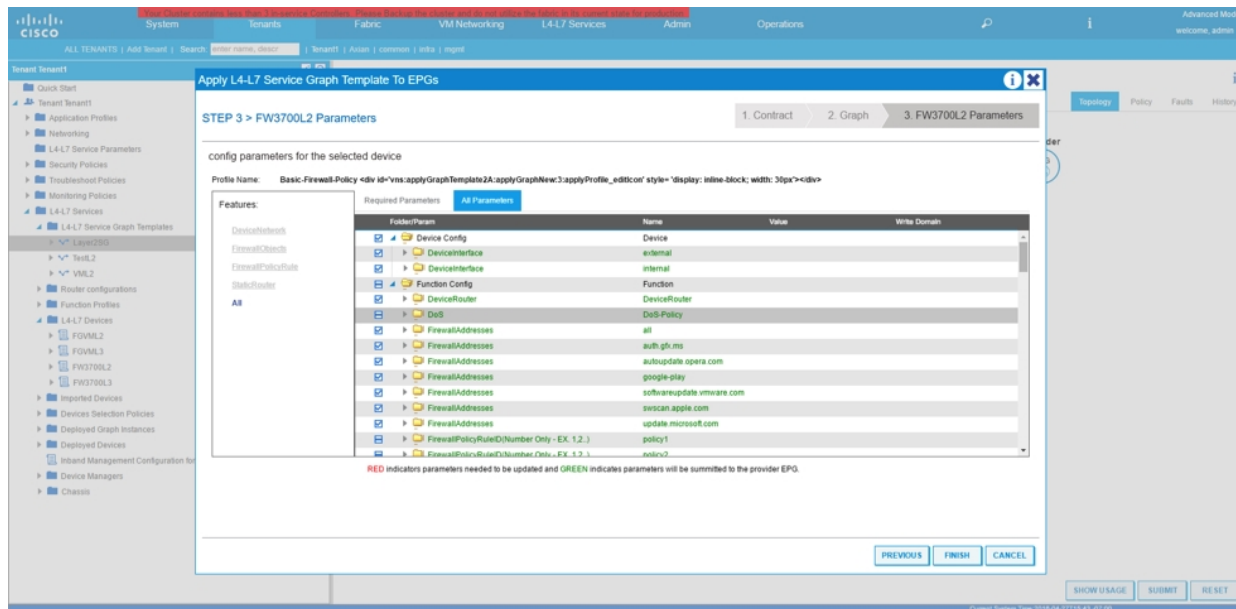
On next screen select the Consumer and provider EPGs and assign a contract name or select a pre-define contract.



Next screen select the logical interfaces defined during the creation of Layer4-7 Device.



Next screen to the last minute check to ensure everything is accordingly before deploy. If ok, then hit the submit button.



Deploy the firewall device shared by multiple service graphs

Pre-requisite

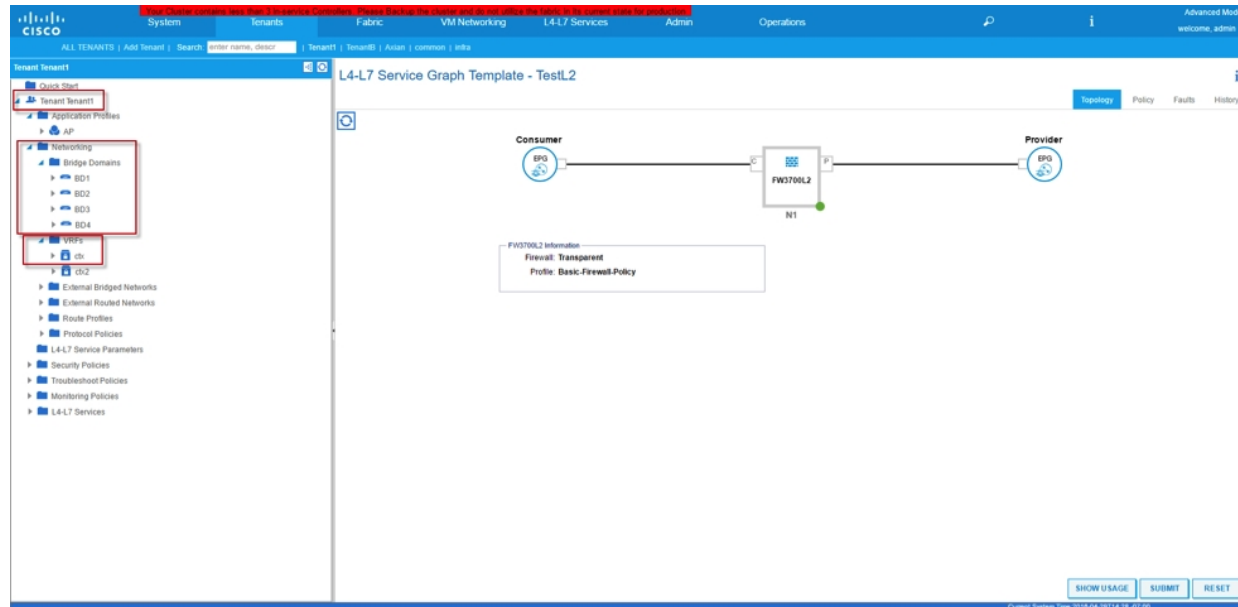
- Fabric Access Policies creation relating to:
 - VLAN Pools
 - Domain
 - Attachable Access Entity Profiles
 - Interface Policies
 - Switch Policies
- Layer4-7 Device Package has imported into Cisco APIC

Work Flow:

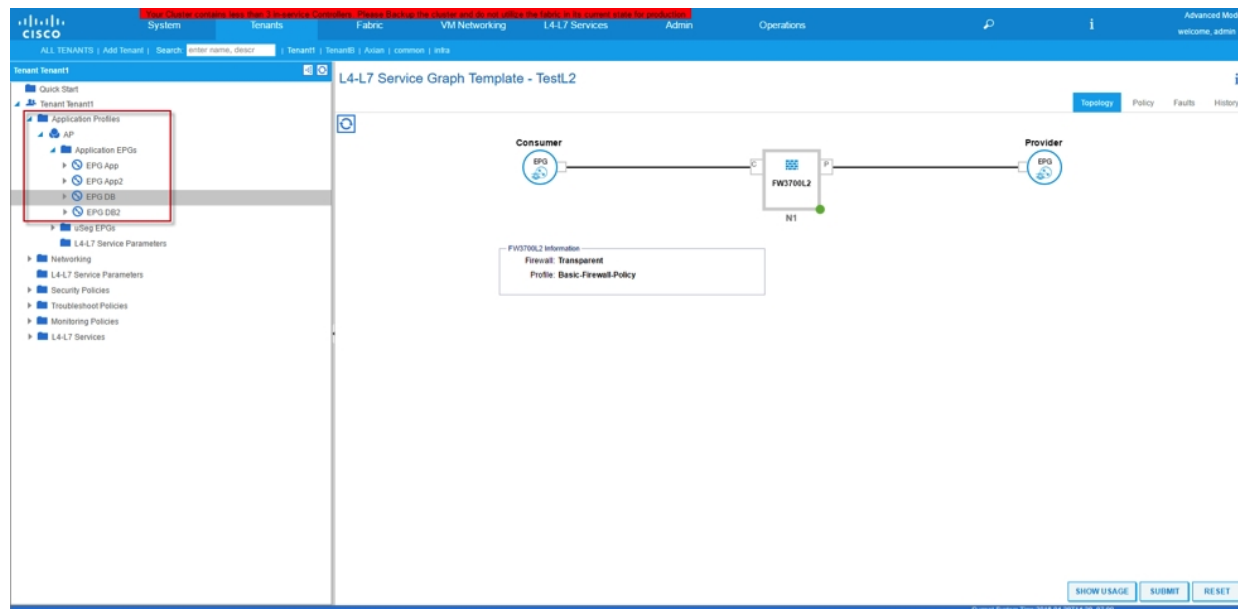
1. Create Tenant ("Tenant1" in our example)
2. Create VRF ("ctx" in our example)
3. Create 4 Bridge Domains ("BD1", "BD2", "BD3" and "BD4" in our example)
4. Associate Bridge Domains to VRF
5. Create 4 EPGs ("App", "App2", "DB", "DB2" in our example)
6. Associate EPGs to Bridge Domains (EPG "App", "App2", "DB" and "DB2" are mapped to Bridge Domain "BD1", "BD2", "BD3" and "BD4" respectively in our example)
7. Create Go-Through mode Device on Cisco APIC and define 4 logical interfaces
8. Create Functional Profile
9. Create 2 Service Graph Templates
10. Deploy Service Graph 2 times on the same device but with different EPG pairs

Configuration

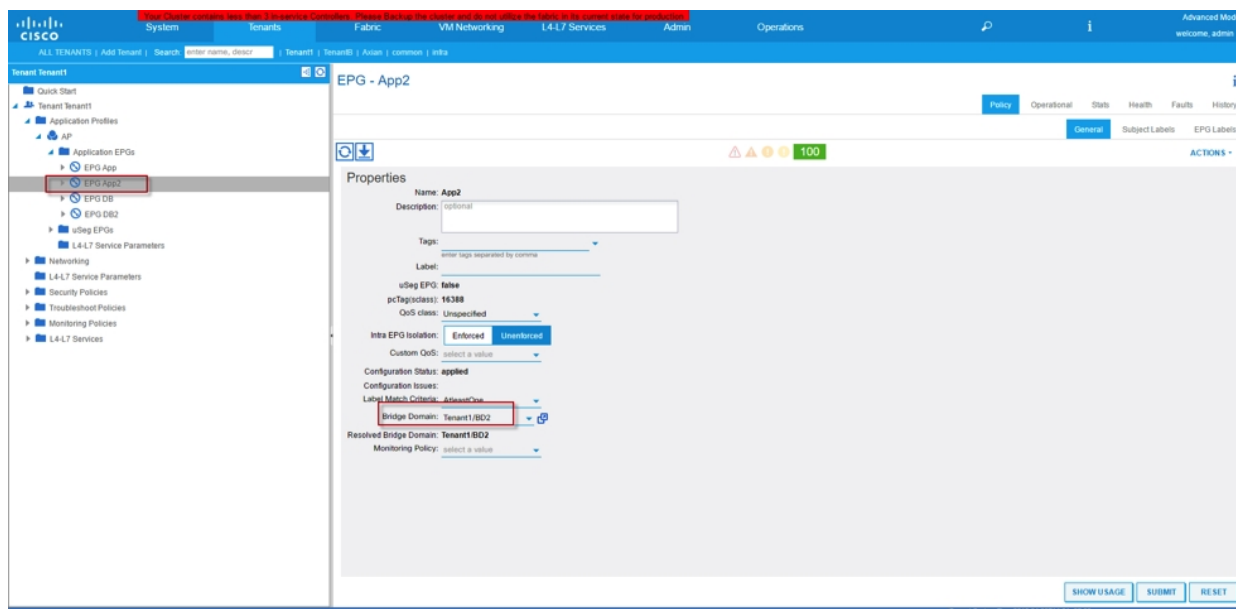
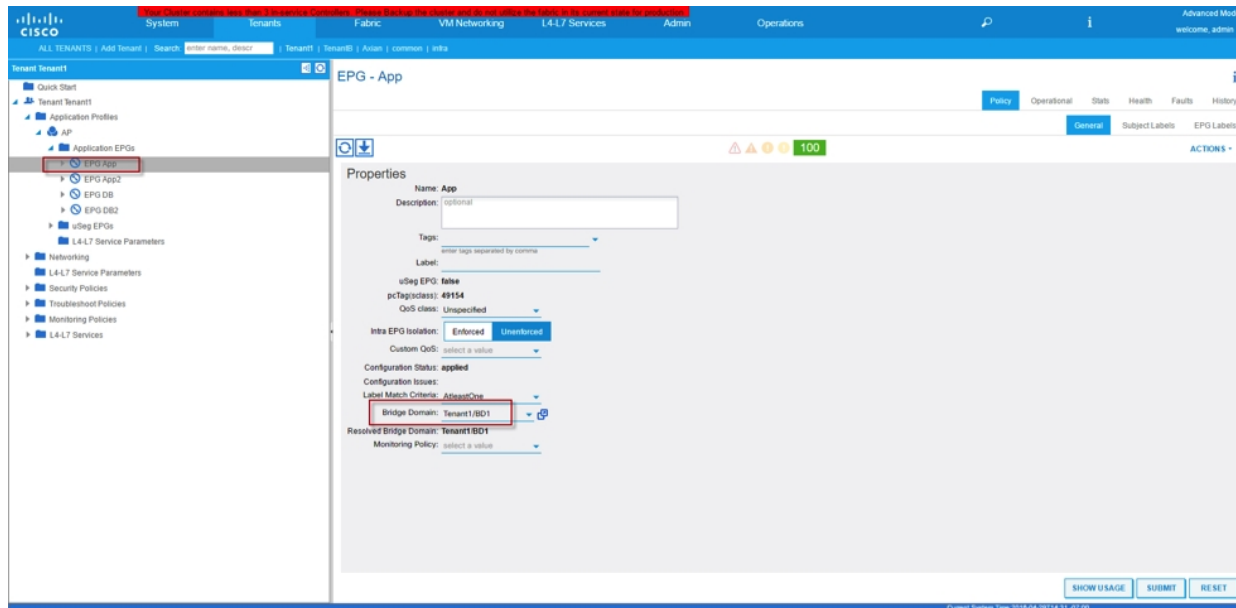
Create Tenant, VRF and 4 Bridge Domains on Cisco APIC

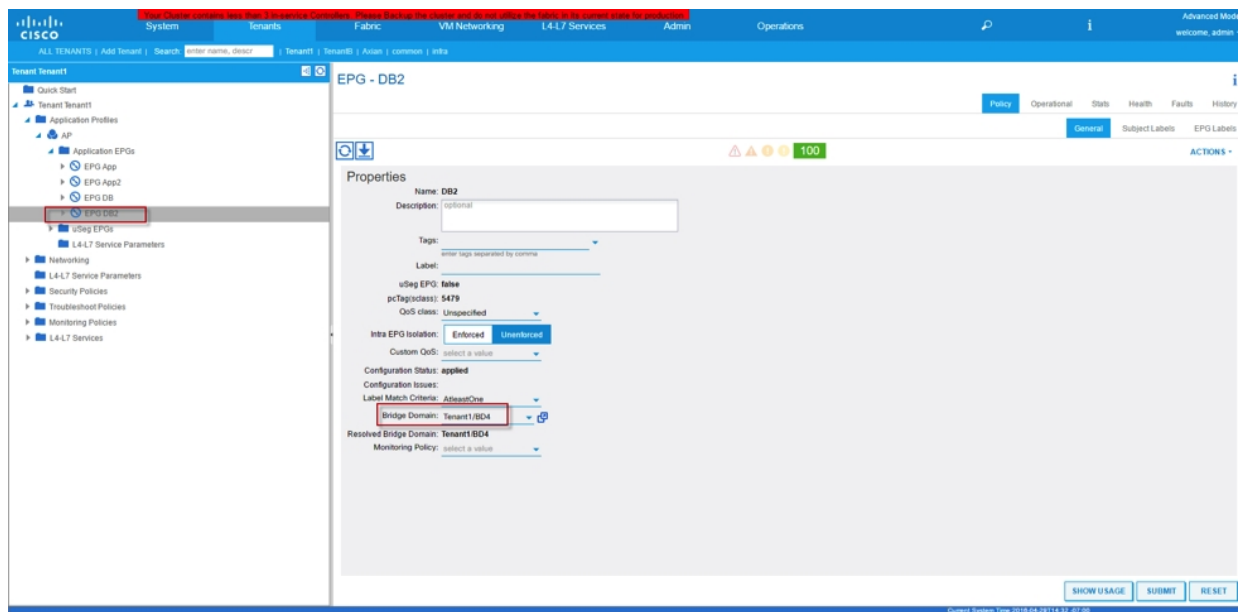
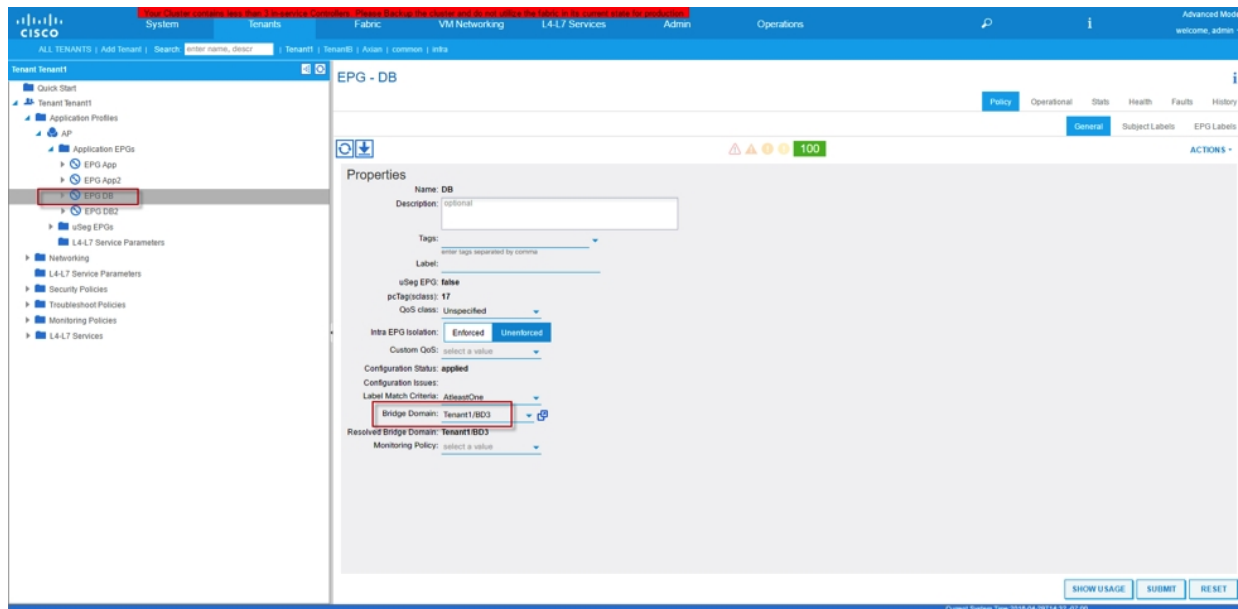


Create 4 EPGs

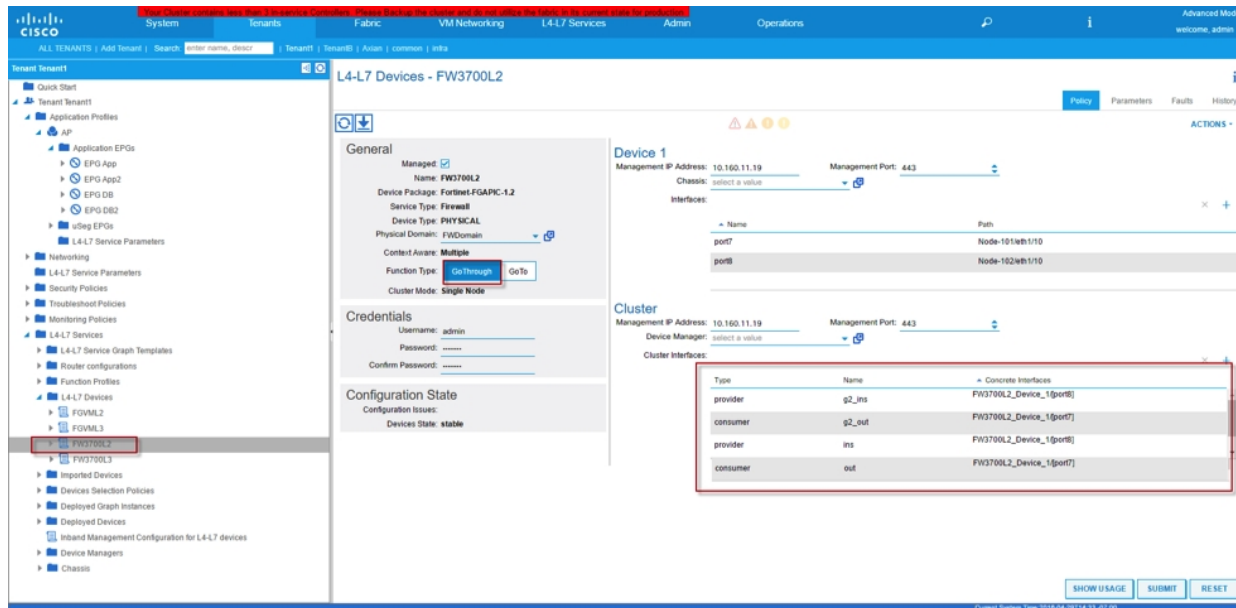


Associate EPG “App”, “App2”, “DB” and “DB2” to Bridge Domain “BD1”, “BD2”, “BD3” and “BD4” respectively



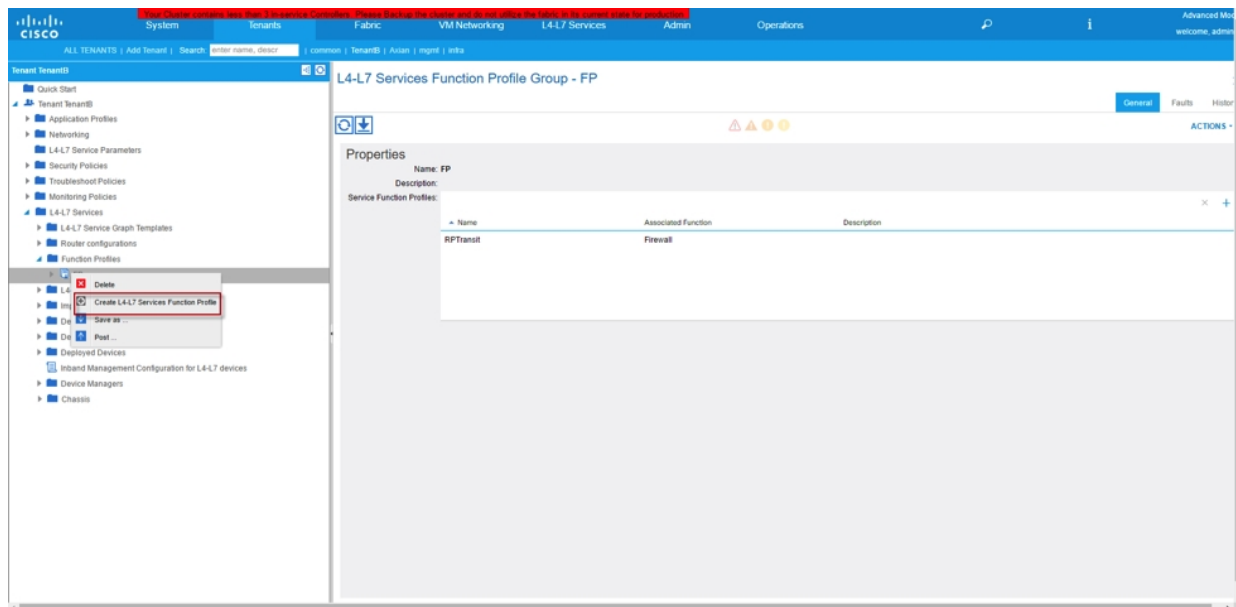


Create Device with Go-Through mode with 4 logical interfaces on Cisco APIC (“Ins” and “Out” for Service Graph 1, “g2_ins” and “g2_out” for Service Graph 2)



Create Functional Profile

Functional Profile defines the template for the Service(s) that is going to deploy such as L4-L7 Device Interface IP addresses, Rule ID, Object Addresses, Policy Rules, Source/Destination Ports...etc.



Functional Profile Objects Explanation

Device Config

Contained External and Internal Interfaces that will be programmed onto Fortigate VDOM. This is the interfaces (typically external and internal) that will be associated to the VDOM. Please leave the field in this section untouched for Go-Through mode deployment.

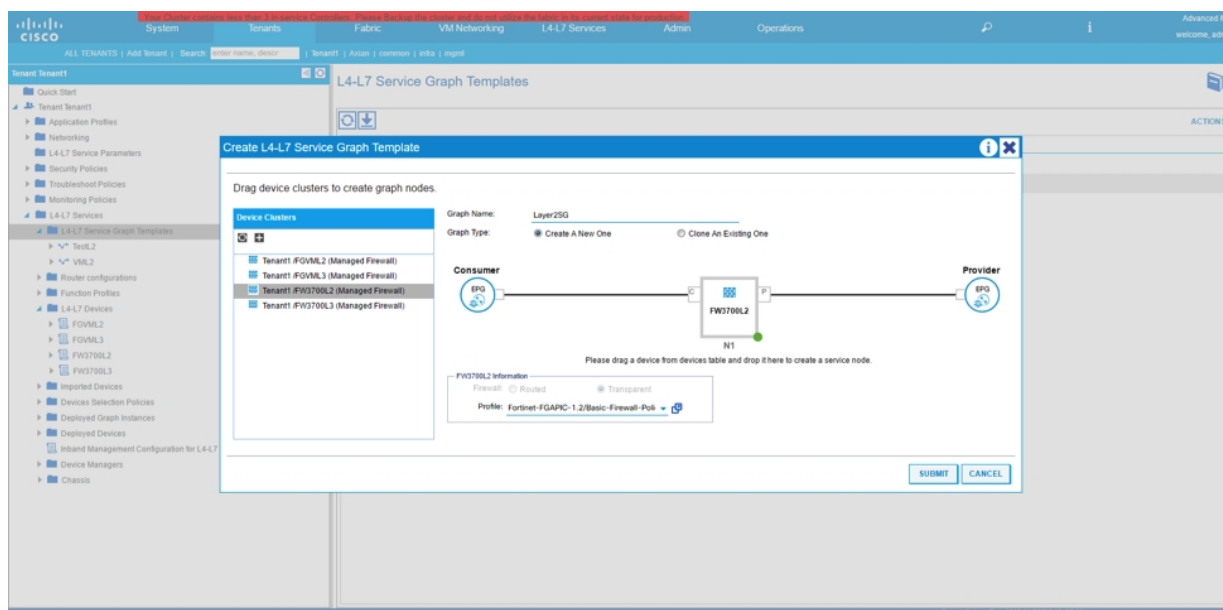
Function Config

Function Config consist of:

- **Network**
 - This field is use for configure Static Routes for IPv4 and IPv6.
- **Policy and Objects**
 - This folder is the container for following list of Folders:
 - a. FWServiceFolder – Firewall Service Object container
 - b. IPv4/IPv6 DoS Policy – Dos Policy configuration
 - c. IPv4/IPv6 FirewallAddresses – Firewall Addresses Object container
 - d. IPv4 Policy – Firewall Policy Rule container
 - e. IPv4 FirewallAddresses Group – Group folder for “Dynamic EPG” feature
 - f. ScheduleFolder – Schedule container
- **VDOM-Folder**
 - VDOM internal and external interfaces

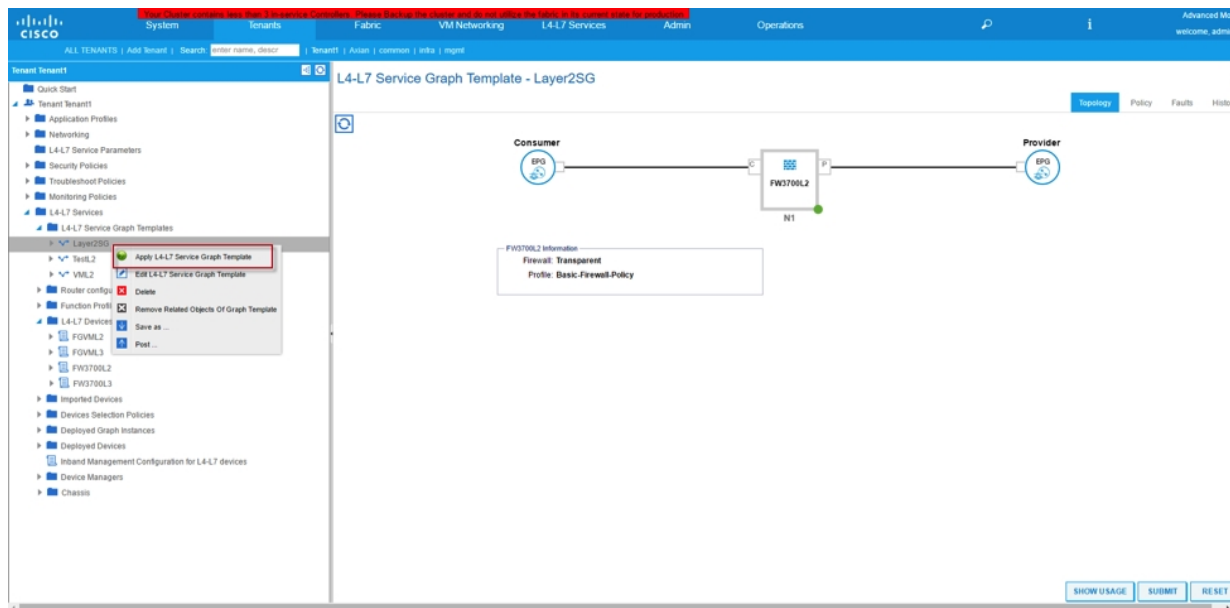
Create Service Graph1

Service Graph template is used to tightly coupled the Functional Profile or Firewall configuration and combine with the Firewall device we defined at earlier steps.

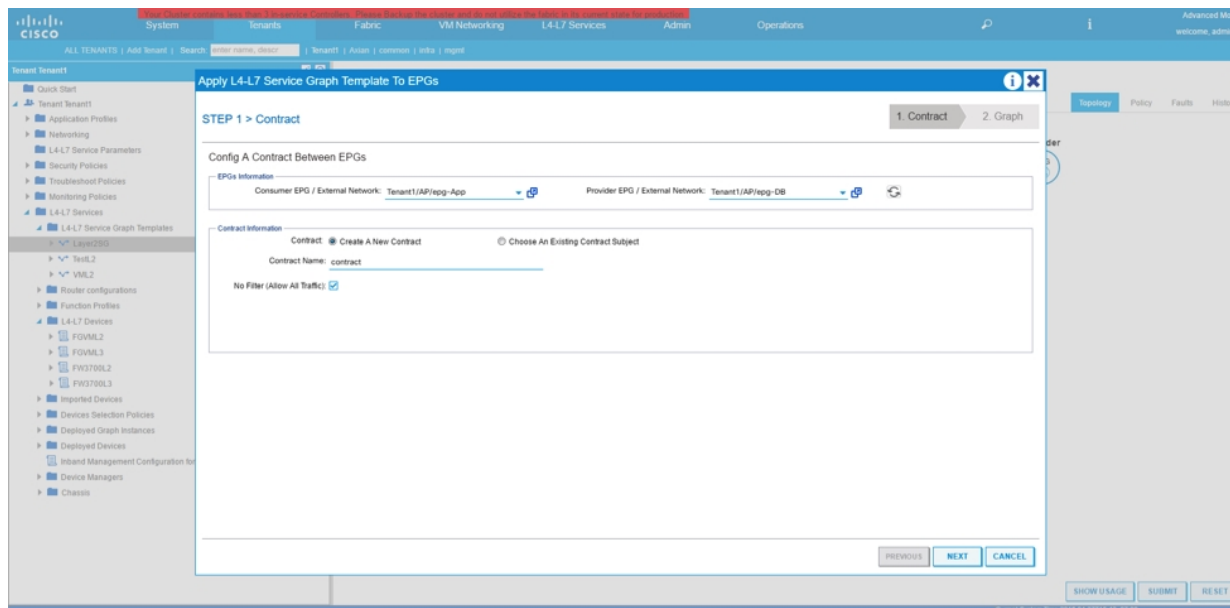


Deploy Service Graph1

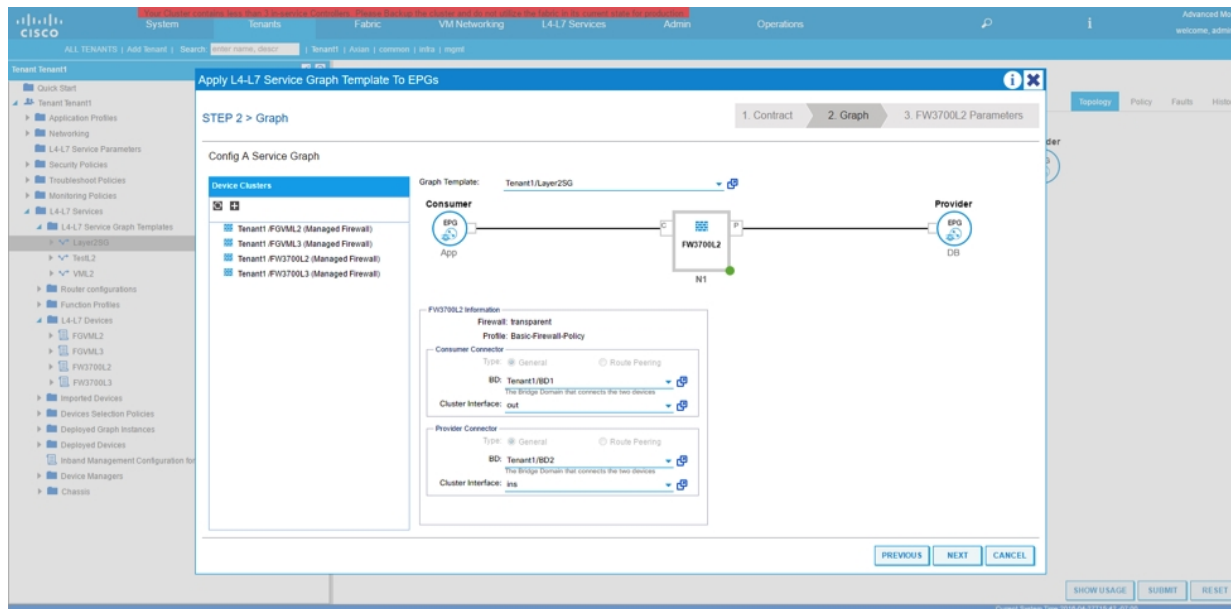
Once we combined the Firewall configuration and associated device together, we are ready to deploy Service Graph 1



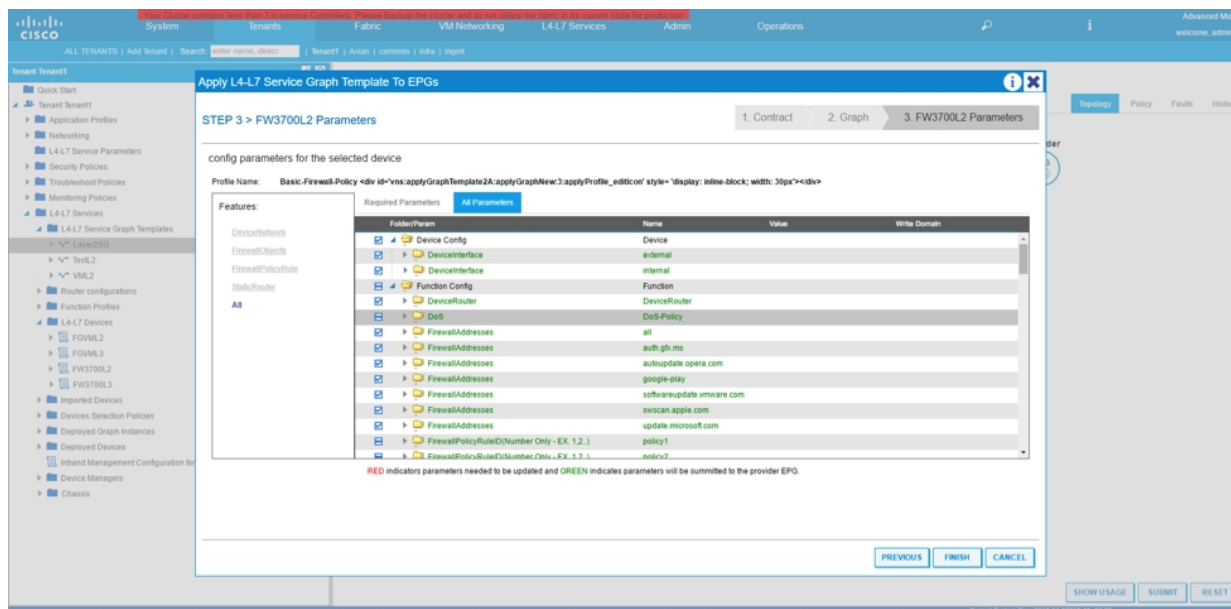
On next screen select the Consumer and provider EPGs (“Apps” and “DB”) and assign a contract name or select a pre-define contract.



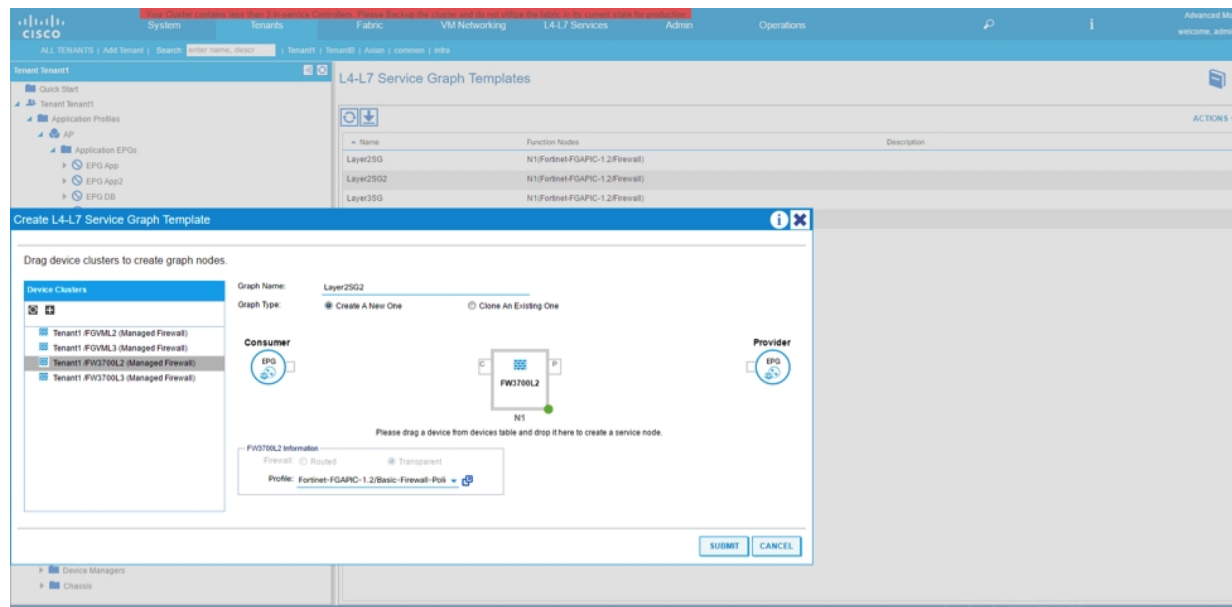
Next screen select the logical interfaces (“ins” and “out”) defined during the creation of Layer4-7 Device.



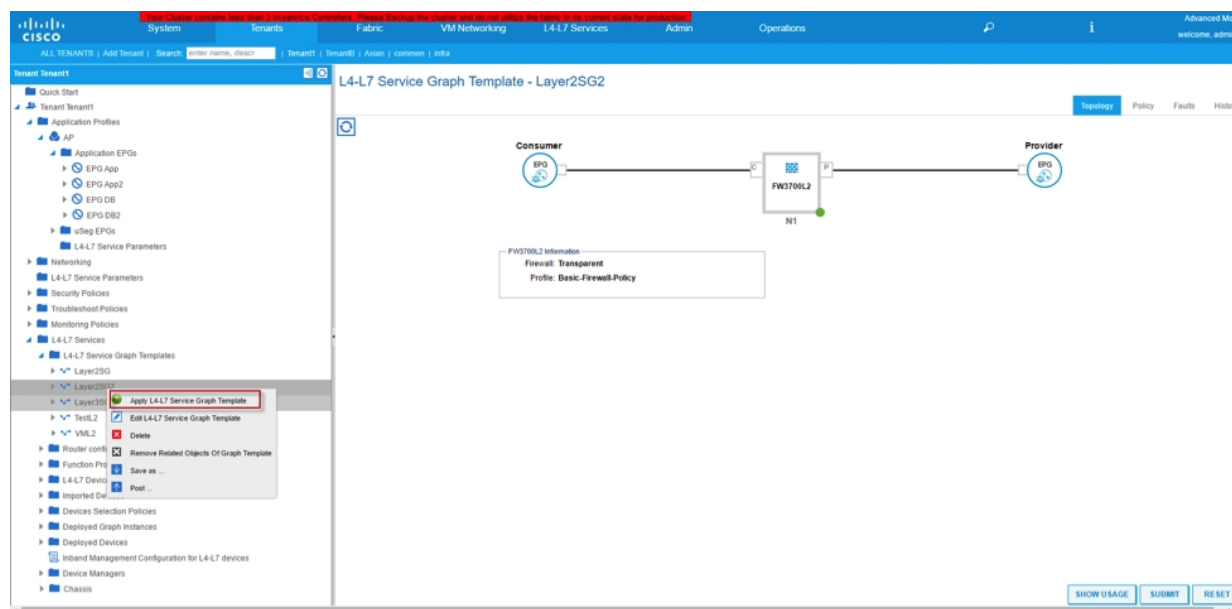
Last minute check to make sure configuration is good before hit “Finish” button



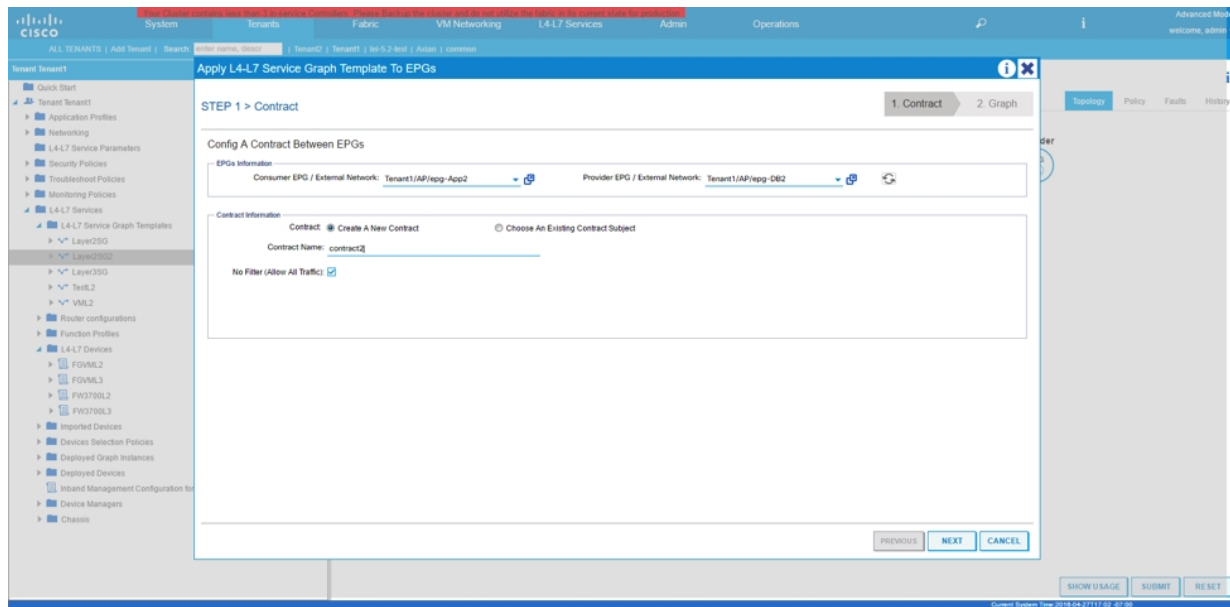
Create Service Graph2



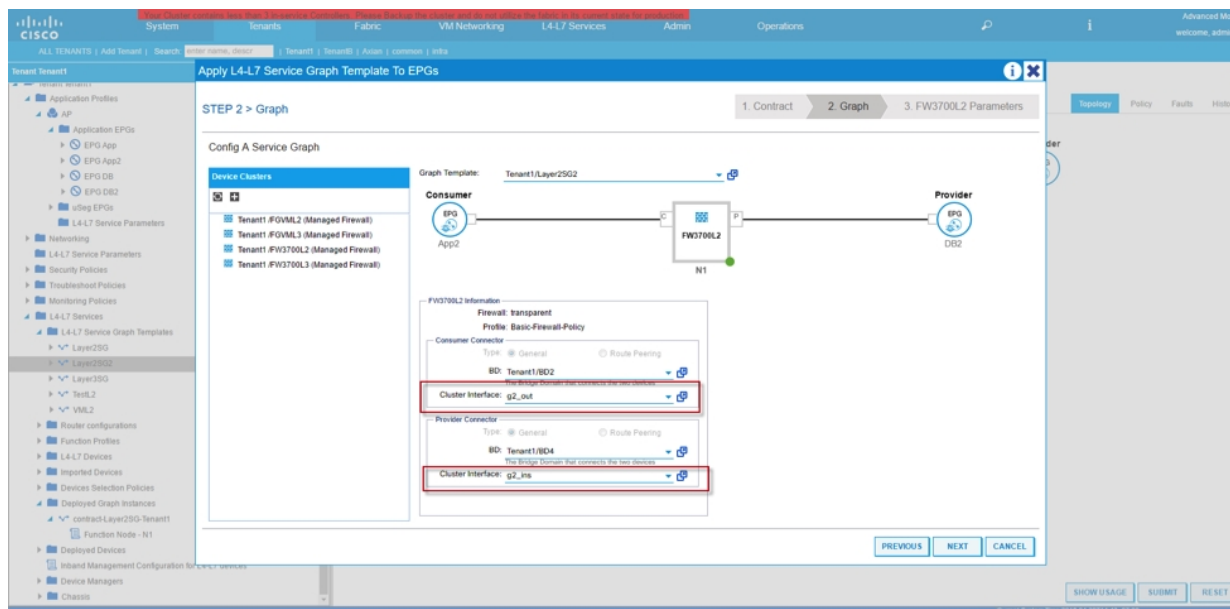
Deploy Service Graph2



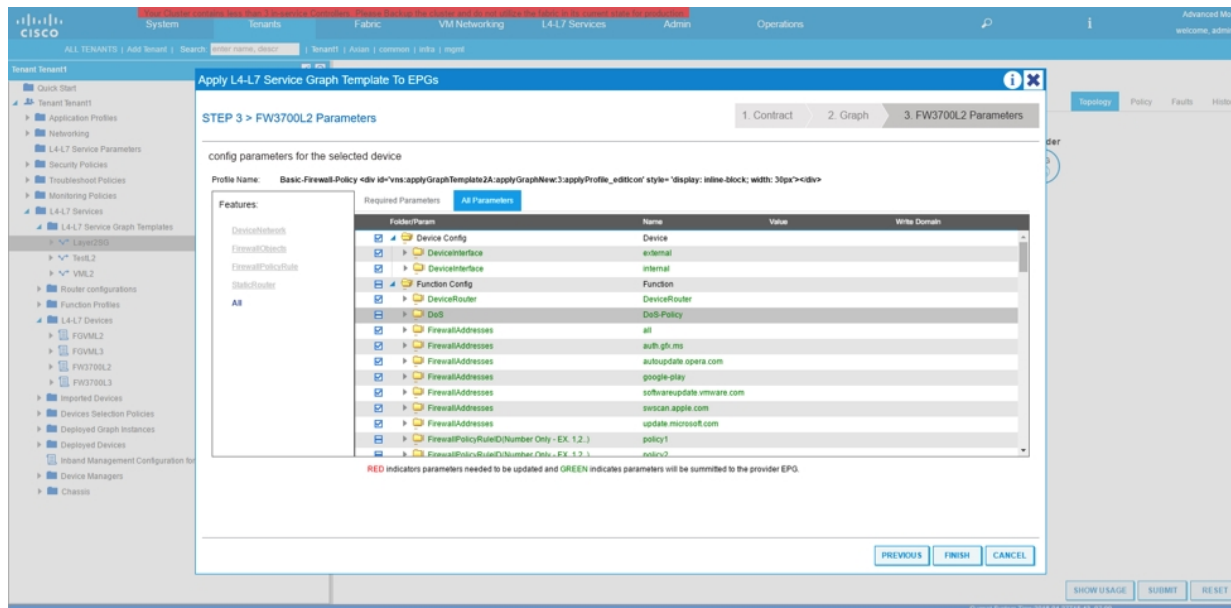
On next screen select the Consumer and provider EPGs (“Apps2” and “DB2”) and assign a contract name or select a pre-define contract.



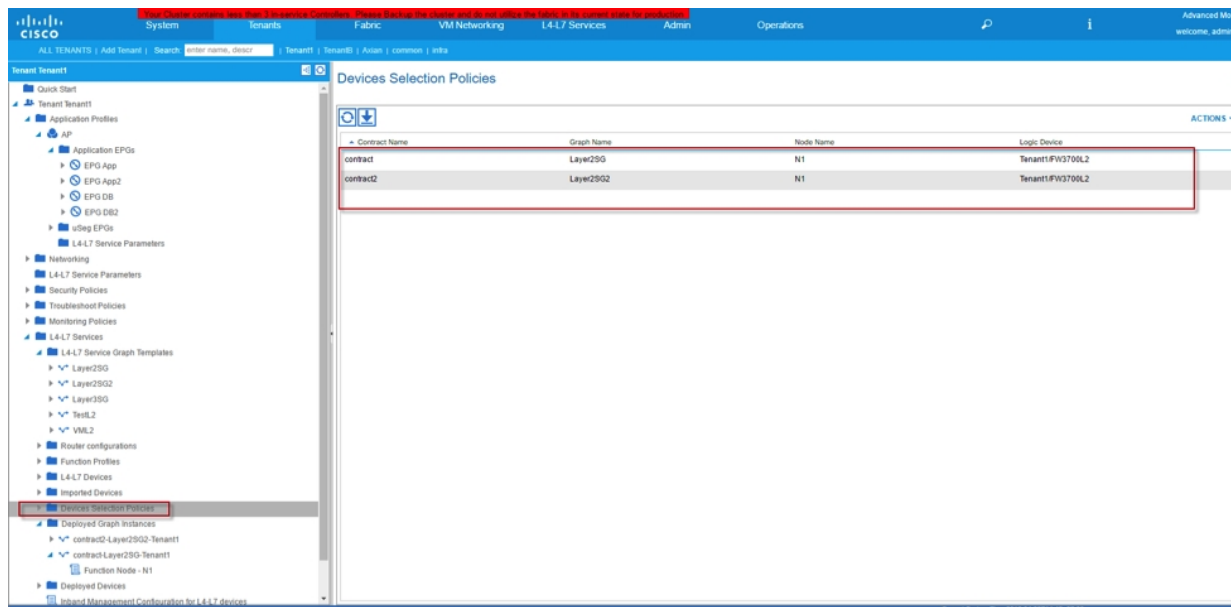
Next screen select the same logical interfaces (g2_ins and g2_out) defined during the creation of Layer 4-7 Device.



Last minute check to make sure configuration is good before hit “Finish” button



Verify Device Selection Policies Creation



Verify Service Graphs Deployment

The screenshot shows the Cisco ACI GUI with the 'Tenant1' tab selected. The left sidebar shows the navigation tree with 'Deployed Graph Instances' highlighted. The main panel displays a table of deployed graph instances.

Service Graph	Contract	Contained By	State	Description
Layer290	contract	Tenant1	applied	
Layer2902	contract2	Tenant1	applied	

The screenshot shows the Cisco ACI GUI with the 'Virtual Device - FW3700L2-ctx' tab selected. The left sidebar shows the navigation tree with 'Deployed Devices' highlighted. The main panel displays the properties of the virtual device.

Properties

Devices: FW3700L2

Virtual Device ID: 5186

VRF: ctx

ACKed Transaction ID: 10002

Current Transaction ID: 10002

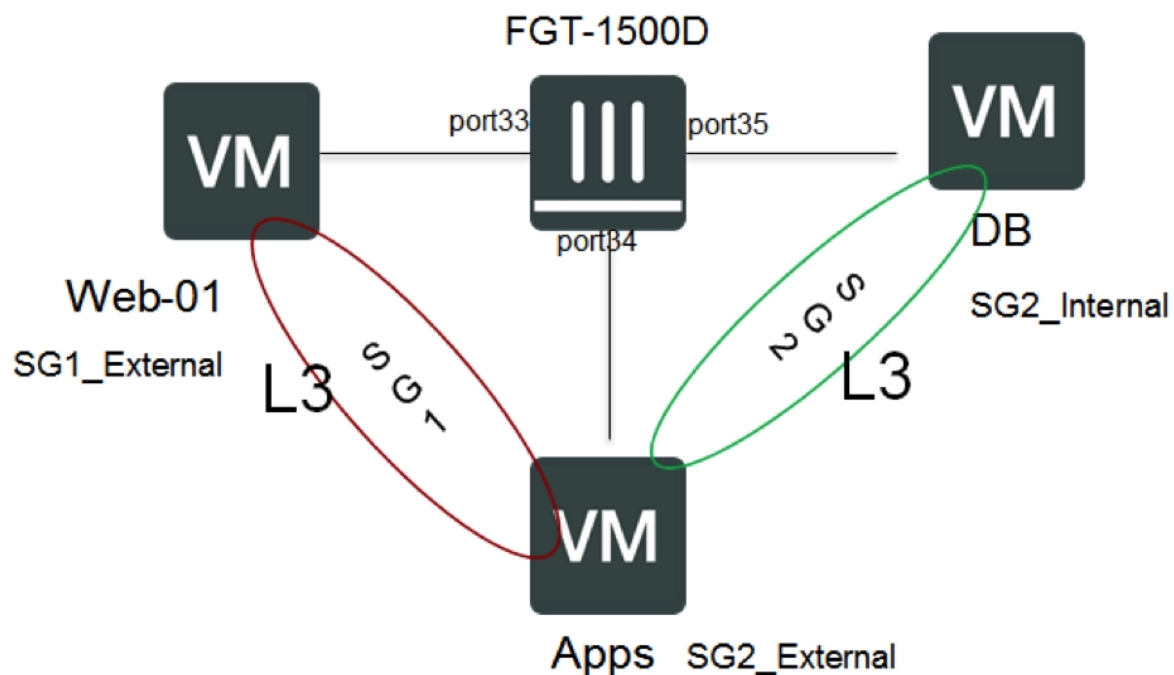
Cluster Interface	Logical Interface	Encap
FW3700L2_g2_in	vlan-1560	
FW3700L2_g2_out	vlan-2748	
FW3700L2_in	vlan-2401	
FW3700L2_out	vlan-2490	

Deploy the firewall device with shared interfaces through multiple service graphs

Pre-requisite

- Fabric Access Policies creation relating to:
 - VLAN Pools
 - Domain
 - Attachable Access Entity Profiles
 - Interface Policies
 - Switch Policies
- Layer4-7 Device Package has imported into Cisco APIC

Basic Topology



Work Flow:

1. Create Tenant ("Demo2" in our example)
2. Create VRF ("vrf1" in our example)
3. Create 3 Bridge Domains ("Web1", "App1", and "DB1" in our example)
4. Associate Bridge Domains to VRF

5. Create 3 EPGs (“Web1”, “App1”, and “DB1” in our example)
6. Associate EPGs to Bridge Domains (EPG “Web1”, “App1”, and “DB1” are mapped to Bridge Domain “Web1”, “App1”, and “DB1” respectively in our example)
7. Create Go-To mode Device on Cisco APIC and define 3 logical interfaces
8. Create Functional Profile
9. Create 2 Service Graph Templates
10. Deploy Service Graph 2 times on the same device but with different EPG pairs

Configuration

Create Tenant, VRF and 3 Bridge Domains on Cisco APIC

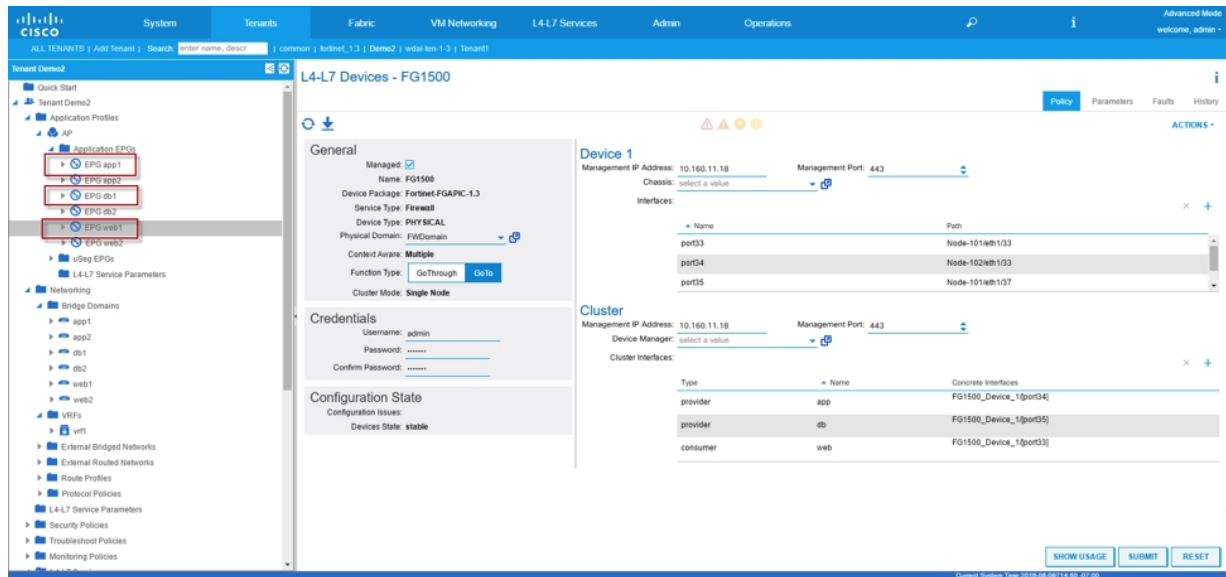
The screenshot displays the Cisco APIC GUI with the following configuration details:

- Tenant (Tenant1):**
 - Application Profiles: EPG app1, EPG app2, EPG db1, EPG db2, EPG web1, EPG web2.
 - Bridge Domains: bd1, bd2, web1, web2.
 - VRFs: vrf1.
- L4-L7 Devices - FG1500:**
 - General:** Managed, Name: FG1500, Device Package: Fortinet-FGAPIC-1.3, Service Type: Firewall, Physical Domain: PHYSICAL, Context Aware: Multiple, Function Type: GoThrough, Cluster Mode: Single Node.
 - Credentials:** Username: admin, Password: (masked), Confirm Password: (masked).
 - Configuration State:** Configuration Issues: 0, Devices State: stable.
- Device 1:**
 - Management IP Address: 10.160.11.18, Management Port: 443.
 - Chassis: select a value.
 - Interfaces:

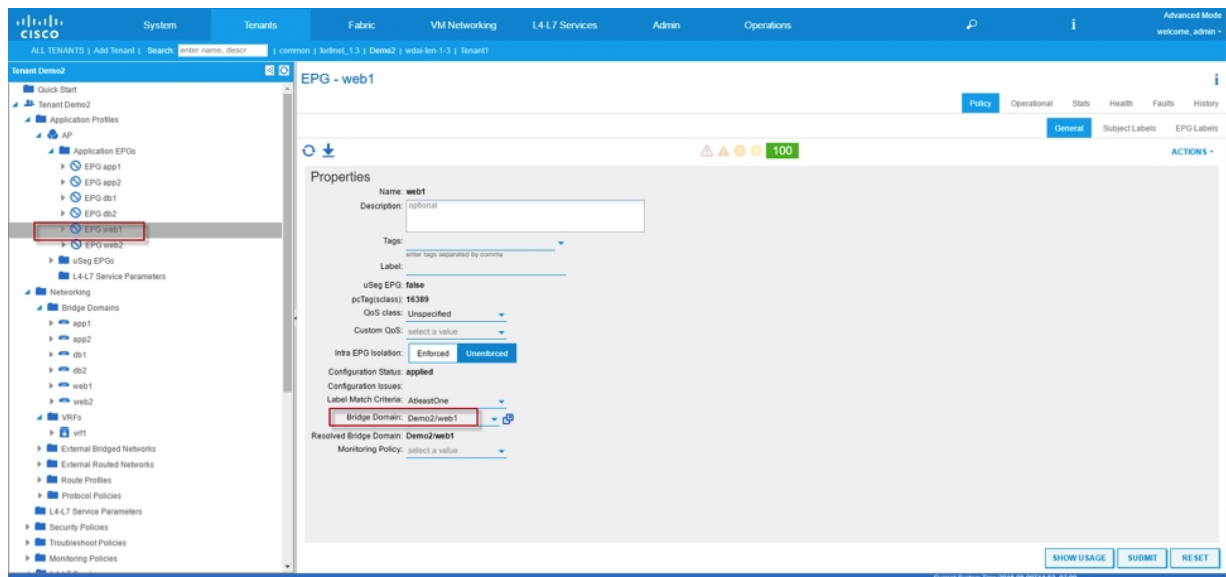
Name	Path
port33	Node-1014eth1/33
port34	Node-1024eth1/33
port35	Node-1014eth1/37
- Cluster:**
 - Management IP Address: 10.160.11.18, Management Port: 443.
 - Device Manager: select a value.
 - Cluster Interfaces:

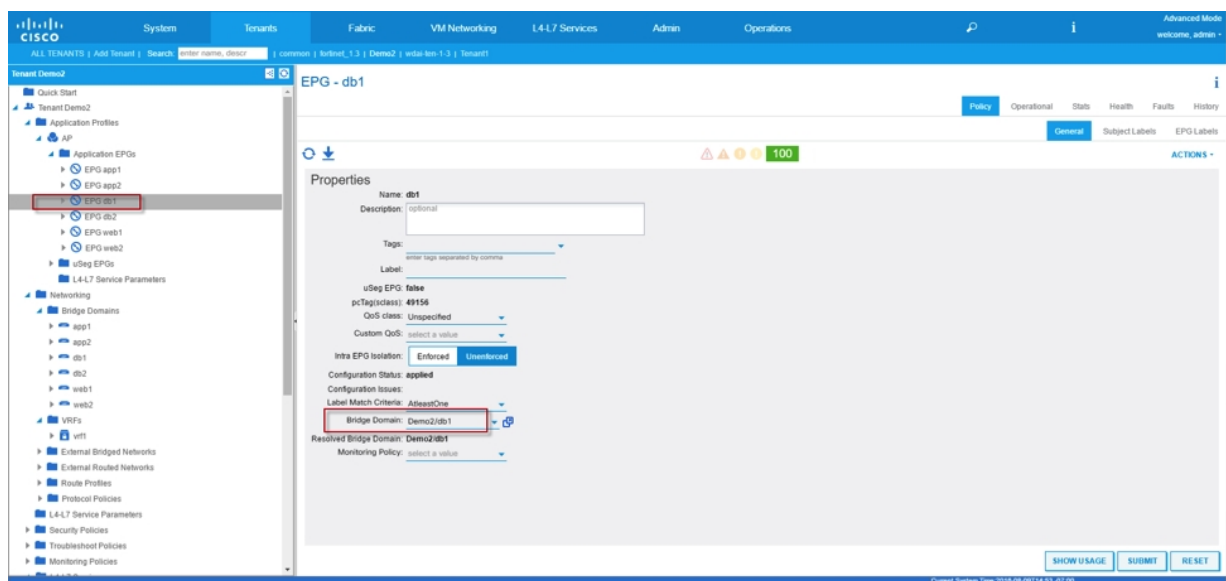
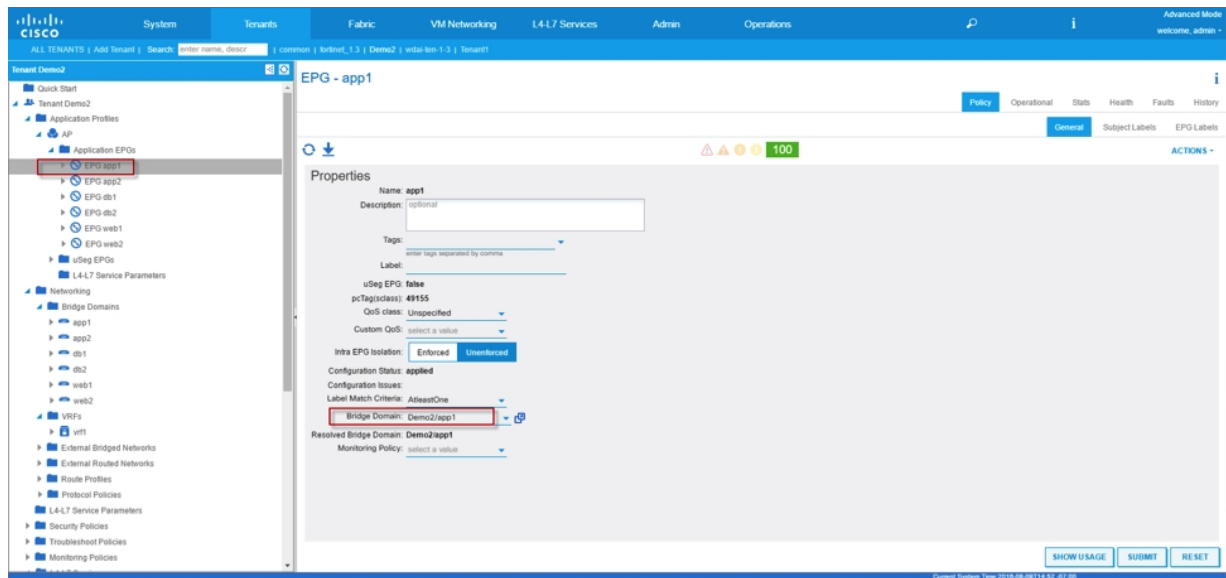
Type	Name	Concrete Interfaces
provider	app	FG1500_Device_1(port34)
provider	db	FG1500_Device_1(port35)
consumer	web	FG1500_Device_1(port33)

Create 3 EPGs



Associate EPG “Web1”, “App1”, and “DB1” to Bridge Domain “Web1”, “App1”, and “DB1” respectively





Create Device with Go-To mode with 3 logical interfaces on Cisco APIC ("Web" "App" and "DB")

The screenshot shows the Cisco APIC GUI with the 'L4-L7 Devices - FG1500' configuration page. The 'General' tab is active, showing the device name 'FG1500', package 'Fortinet-FGAPIC-1.3', and service type 'Firewall'. The 'Function Type' is set to 'GoThrough' and 'Cluster Mode' is 'Single Node'. The 'Cluster' tab shows the device manager and cluster interfaces. The cluster interfaces table is as follows:

Type	Name	Concrete Interfaces
provider	app	FG1500_Device_1(port34)
provider	db	FG1500_Device_1(port35)
consumer	web	FG1500_Device_1(port33)

Create Functional Profile

Functional Profile defines the template for the Service(s) that is going to deploy such as L4-L7 Device Interface IP addresses, Rule ID, Object Addresses, Policy Rules, Source/Destination Ports...etc.

The screenshot shows the Cisco APIC GUI with the 'L4-L7 Services Function Profile Group - FP' configuration page. The 'Properties' tab is active, showing the name 'FP' and description. The 'Service Function Profiles' table is as follows:

Name	Associated Function	Description
AppToDB	Firewall	
AppToWeb	Firewall	

Functional Profile Objects Explanation:

Device Config

Contains External and Internal Interfaces that will be programmed onto Fortigate VDOM. This is the interfaces (typically external and internal) that will be associated to the VDOM. Please leave the field in this section untouched for Go-Through mode deployment.

Function Config

Function Config consist of:

- **Network**
 - This field is use for configure Static Routes for IPv4 and IPv6.
- **Policy and Objects**
 - This folder is the container for following list of Folders:
 - a. FWServiceFolder – Firewall Service Object container
 - b. IPv4/IPv6 DoS Policy – Dos Policy configuration
 - c. IPv4/IPv6 FirewallAddresses – Firewall Addresses Object container
 - d. IPv4 Policy – Firewall Policy Rule container
 - e. IPv4 FirewallAddresses Group – Group folder for “Dynamic EPG” feature
 - f. ScheduleFolder – Schedule container
- **VDOM-Folder**
 - VDOM internal and external interfaces

Beginning with this release, we allow the change of DeviceInterface name and the default is External/Internal. Please see below screenshot where we changed the DeviceInterface name from External/Internal to app/web respectively.

The screenshot displays the Cisco ACI GUI for the 'L4-L7 Services Function Profile - AppToWeb'. The 'Properties' section shows the name 'AppToWeb' and the associated function 'Fortinet-FGAPIC-1.3Firewall'. The 'FEATURES AND PARAMETERS' section includes a table for 'DeviceInterface' with the following data:

Feature	Name	Value	Mandatory	Locked	Shared
Device Config	Device				
DeviceInterface	app		false	false	false
DeviceInterface	web		false	false	false
Function Config	Function				
Network	Network		false	false	false
Policy and Objects	PolicyObjects		false	false	false
VDOM-Folder	vdome-folder		false	false	false

In addition, for this use case scenario, App is going to be the shared interface between the two service graphs, therefore it is crucial that the DeviceInterface name and the content are identical across both service graphs.

Please see screenshot for “app” between two service graphs (ApptoWeb and ApptoDB).

The screenshot shows the Cisco ACI GUI for the 'L4-L7 Services Function Profile - ApptoWeb'. The left sidebar shows the navigation tree with 'ApptoWeb' selected. The main panel displays the 'Properties' and 'FEATURES AND PARAMETERS' sections. The 'DeviceInterface' section is highlighted with a red box, showing the 'app' interface configuration.

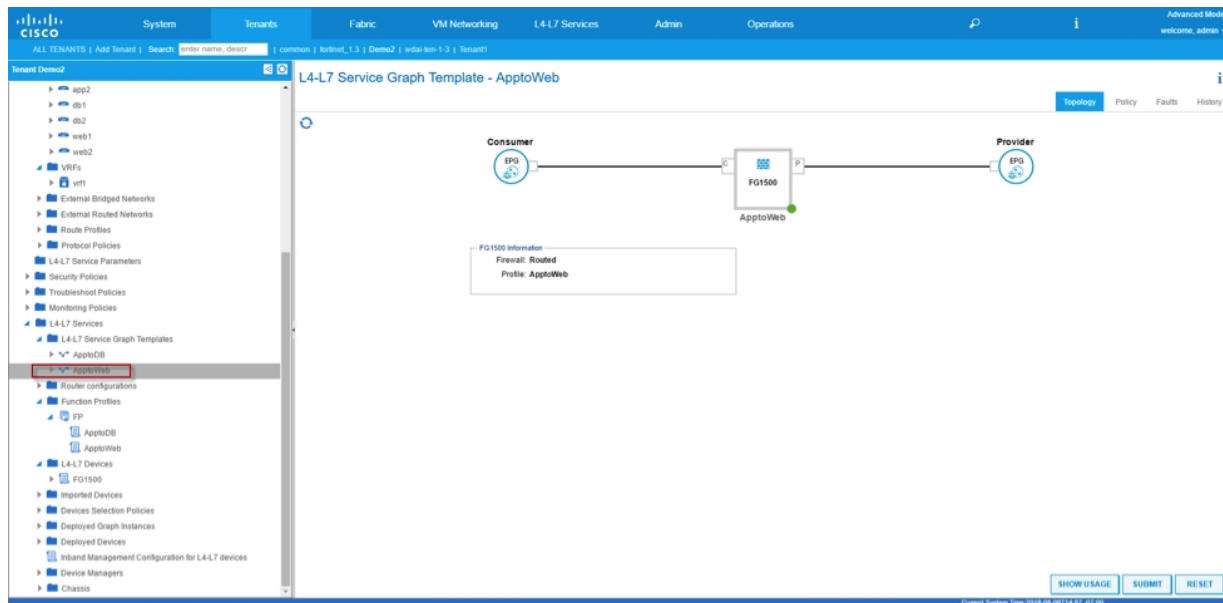
Meta Folder/Parent Key	Name	Value	Mandatory	Locked	Shared
DeviceInterface	app			false	false
DeviceInterface	Device			false	false
DeviceInterface	AllowAccess			false	false
DeviceInterface	Device IP Address(es): 10.160.11.1 or 0.0.0.0 (transparent)	IPAddress	10.0.2.1	false	false
DeviceInterface	Device IP Netmask(s): 255.255.255.0	IPNetmask	255.255.255.0	false	false
DeviceInterface	Device IPv6 Address(es): -	IPv6Address	-	false	false
DeviceInterface	Device IPv6 Netmask(s): 0	IPv6Netmask	0	false	false
DeviceInterface	Interface IPv6 Address Mode(static, dhcp, pppoe)	IPv6Mode	static	false	false
DeviceInterface	Interface Address Mode(static, dhcp, pppoe)	mode	static	false	false
DeviceInterface	DeviceInterface	web		false	false
Function Config	Function			false	false
Network	Network			false	false
Policy and Objects	PolicyObjects			false	false
VDOM Folder	vdome-folder			false	false

The screenshot shows the Cisco ACI GUI for the 'L4-L7 Services Function Profile - ApptoDB'. The left sidebar shows the navigation tree with 'ApptoDB' selected. The main panel displays the 'Properties' and 'FEATURES AND PARAMETERS' sections. The 'DeviceInterface' section is highlighted with a red box, showing the 'app' interface configuration.

Meta Folder/Parent Key	Name	Value	Mandatory	Locked	Shared
DeviceInterface	app			false	false
DeviceInterface	Device			false	false
DeviceInterface	AllowAccess			false	false
DeviceInterface	Device IP Address(es): 10.160.11.1 or 0.0.0.0 (transparent)	IPAddress	10.0.2.1	false	false
DeviceInterface	Device IP Netmask(s): 255.255.255.0	IPNetmask	255.255.255.0	false	false
DeviceInterface	Device IPv6 Address(es): -	IPv6Address	-	false	false
DeviceInterface	Device IPv6 Netmask(s): 0	IPv6Netmask	0	false	false
DeviceInterface	Interface IPv6 Address Mode(static, dhcp, pppoe)	IPv6Mode	static	false	false
DeviceInterface	Interface Address Mode(static, dhcp, pppoe)	mode	static	false	false
DeviceInterface	DeviceInterface	db		false	false
Function Config	Function			false	false
Network	Network			false	false
Policy and Objects	PolicyObjects			false	false
VDOM Folder	vdome-folder			false	false

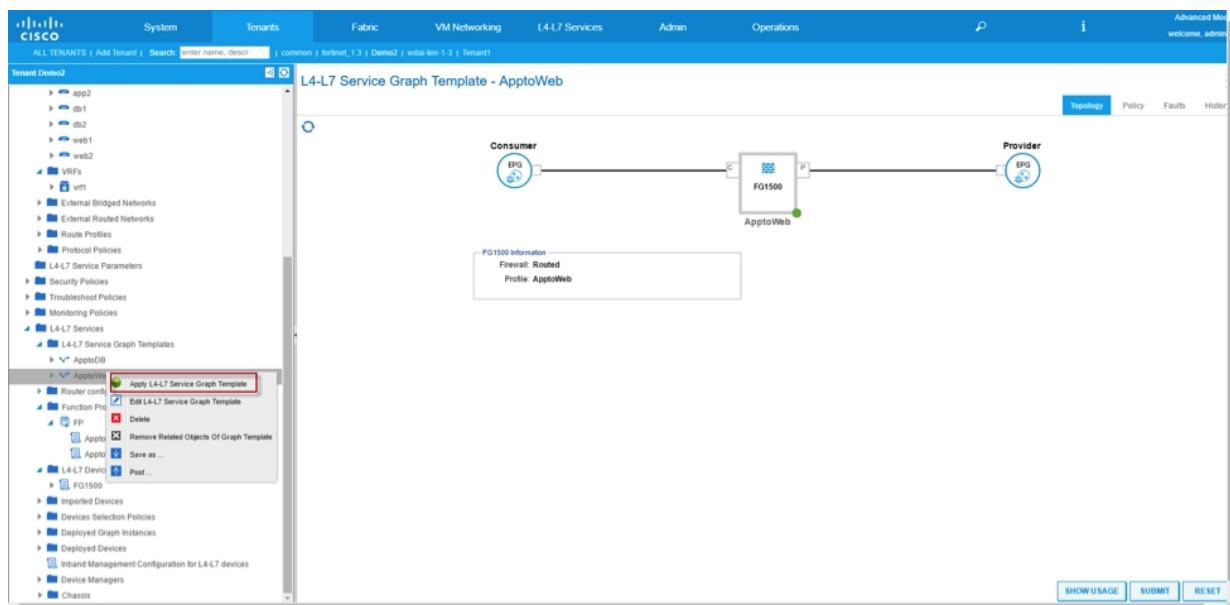
Create Service Graph1 for Web1 and App1

Service Graph template is used to tightly coupled the Functional Profile or Firewall configuration and combine with the Firewall device we defined at earlier steps.

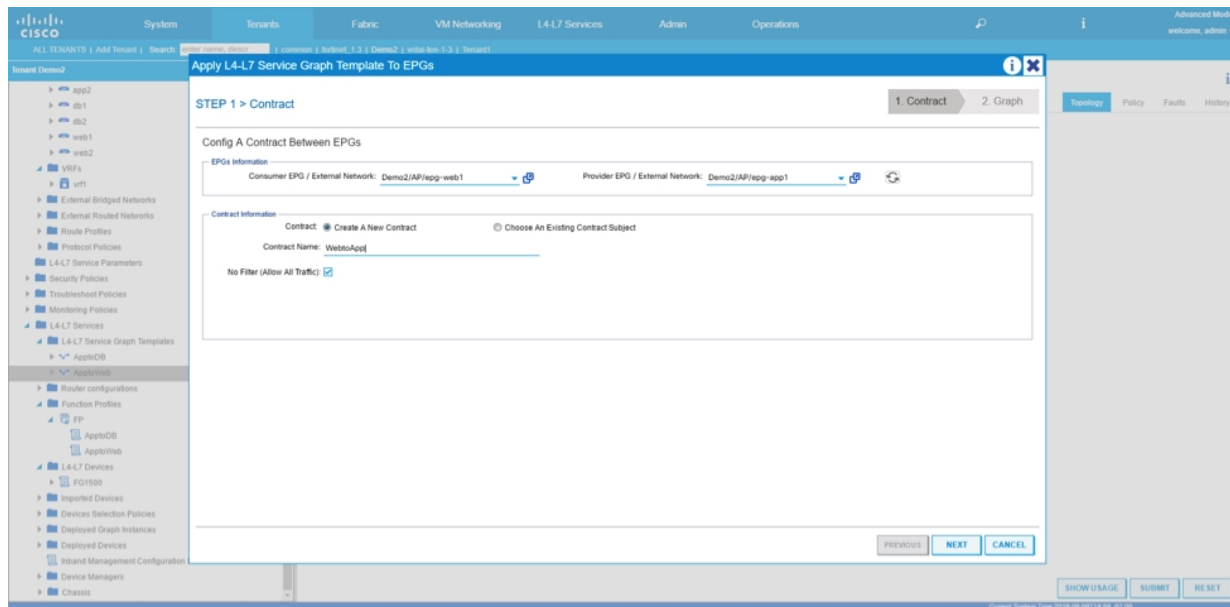


Deploy Service Graph1 Web1 to App1

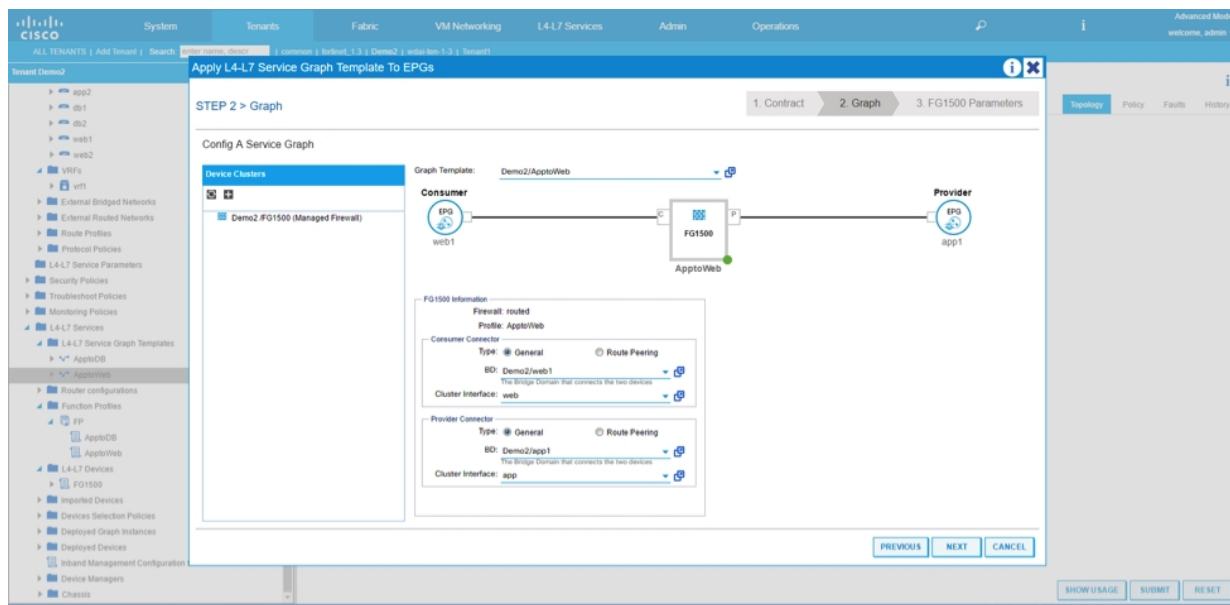
Once we combined the Firewall configuration and associated device together, we are ready to deploy Service Graph 1



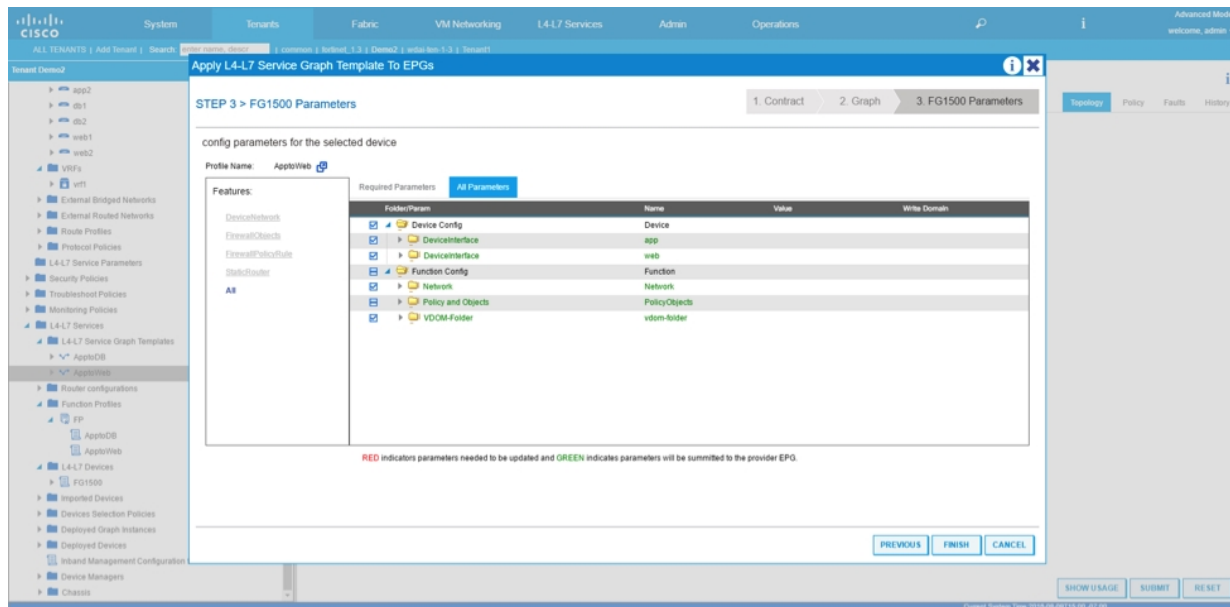
On next screen select the Consumer and provider EPGs ("Web1" and "App1") and assign a contract name or select a pre-define contract.



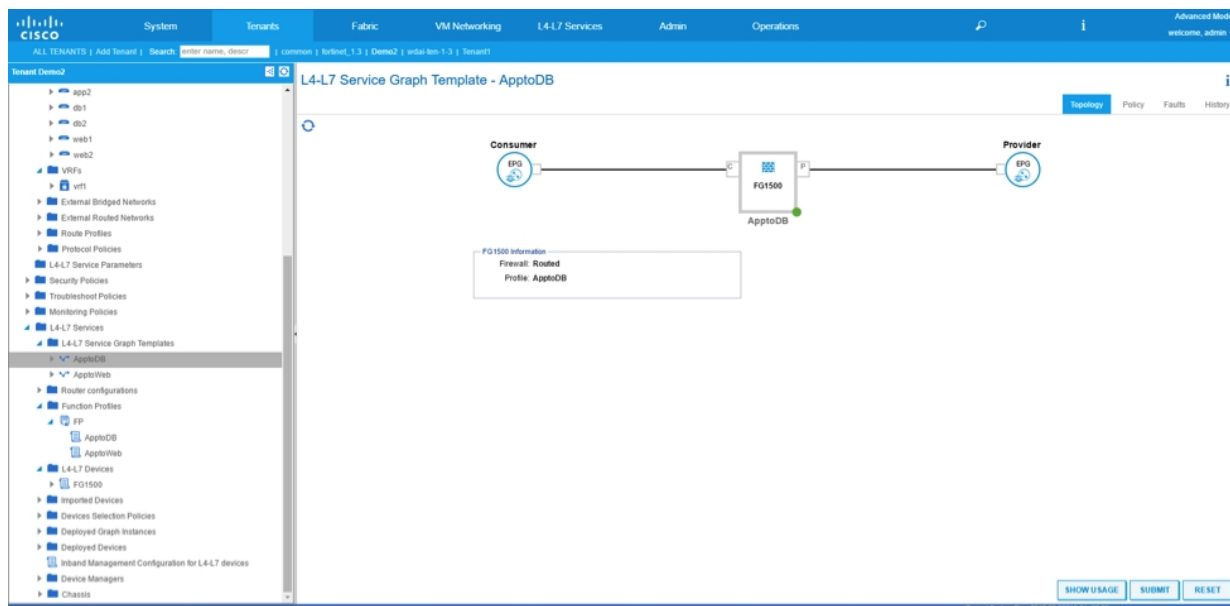
Next screen select the logical interfaces (“app” and “web”) defined during the creation of Layer4-7 Device.



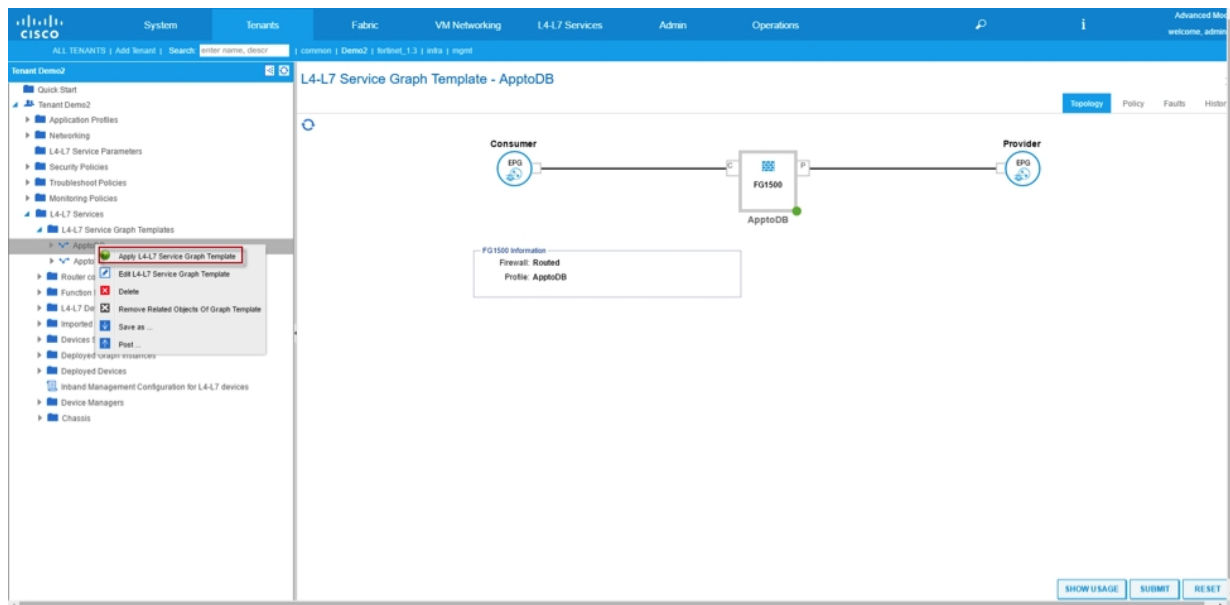
Last minute check to make sure configuration is good before hit “Finish” button



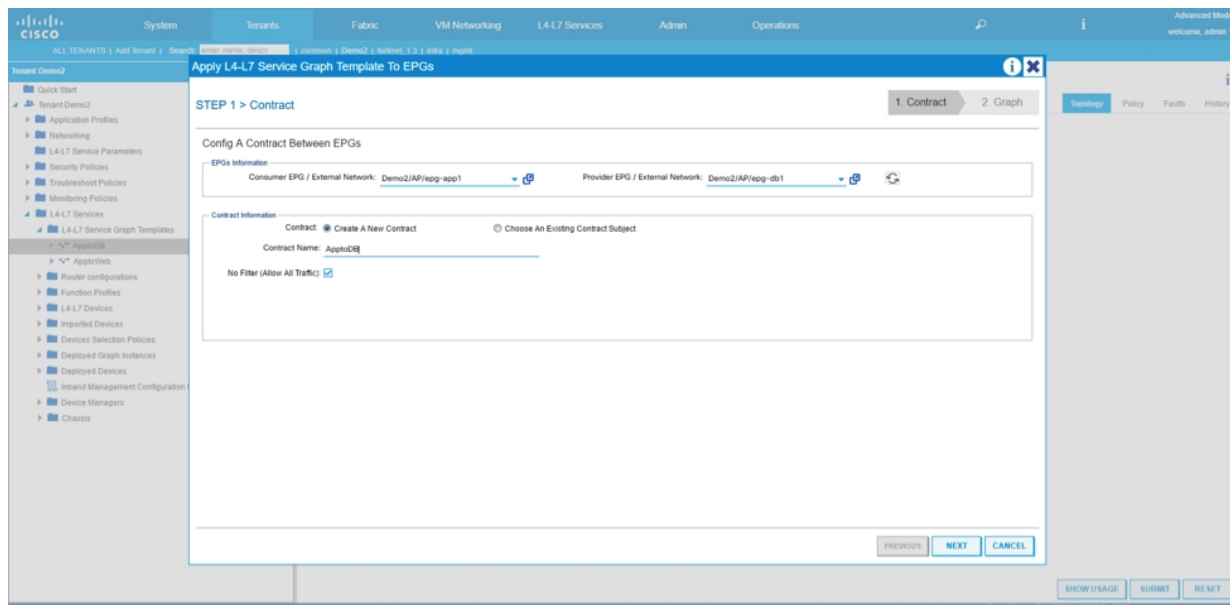
Create Service Graph2 App1 to DB1



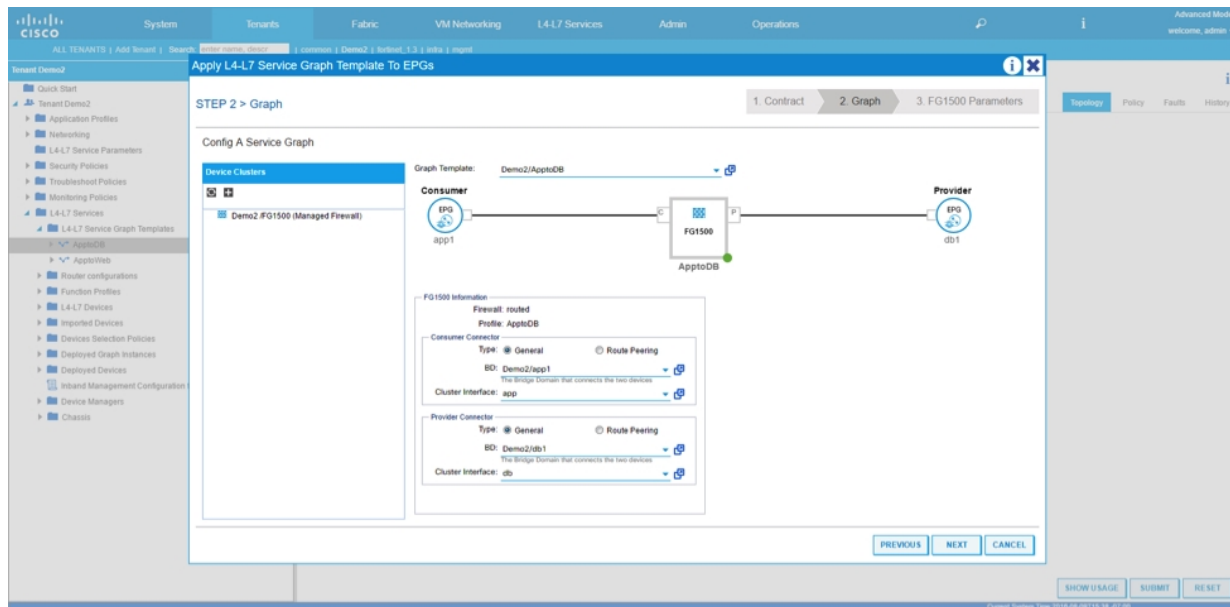
Deploy Service Graph2 App1 to DB1



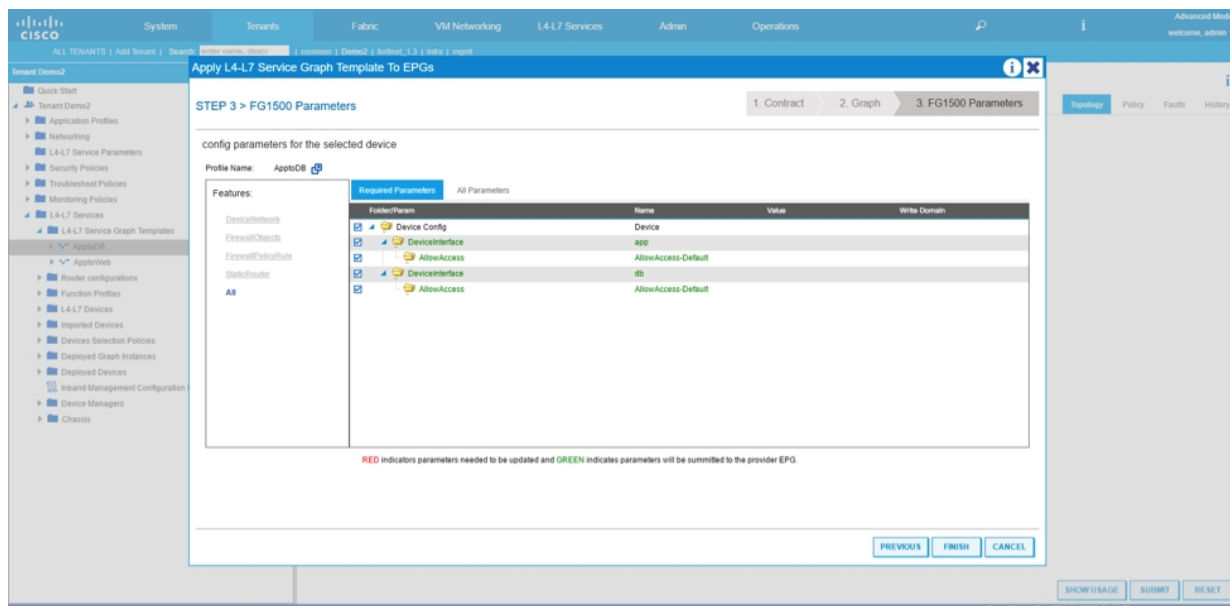
On next screen select the Consumer and provider EPGs ("App1" and "DB1") and assign a contract name or select a pre-define contract.



Next screen select the logical interfaces (App and DB) defined during the creation of Layer4-7 Device.



Last minute check to make sure configuration is good before hit “Finish” button



Verify Device Selection Policies Creation

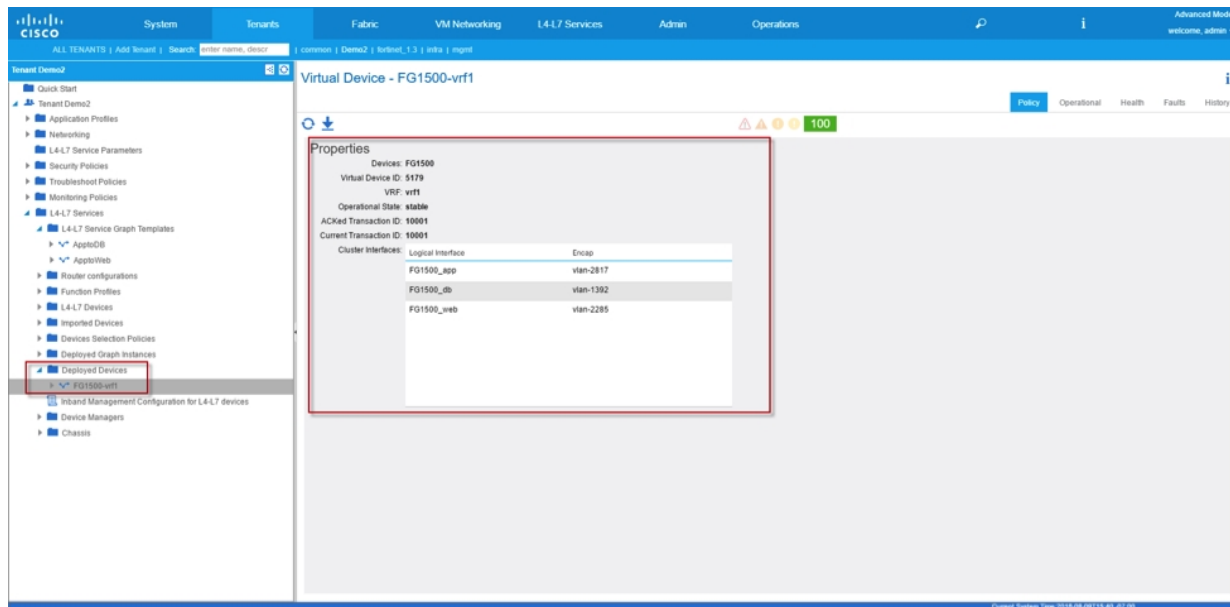
Devices Selection Policies

Contract Name	Graph Name	Node Name	Logic Device
AppToDB	AppToDB	AppToDB	Demo2FG1500
AppToWeb	AppToWeb	AppToWeb	Demo2FG1500

Verify Service Graphs Deployment

Deployed Graph Instances

Service Graph	Contract	Contained By	State	Description
AppToWeb	AppToWeb	Tenant Demo2	applied	
AppToDB	AppToDB	Tenant Demo2	applied	



Deploy the firewall device in a one-arm configuration with policy based redirect

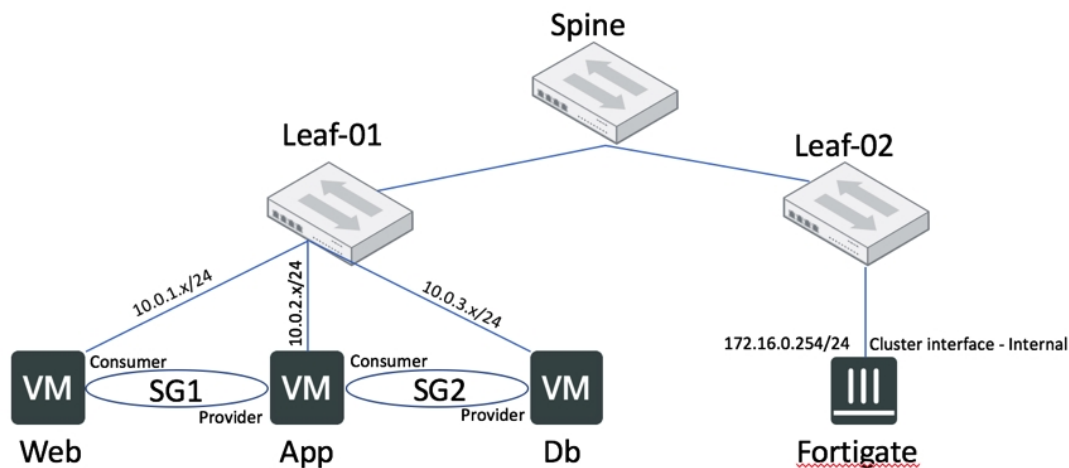
Prerequisites

- Fabric Access Policies creation relating to:
 - VLAN Pools
 - Domain
 - Attachable Access Entity Profiles
 - Interface Policies
 - Switch Policies
- Layer 4-7 Device Package has been imported into Cisco APIC
- Layer 4-7 Policy Based Redirect required (Cisco ACI 2.x above)
- Dynamic EPG Notification (optional)
- Separate Firewall Bridge Domain. Required for Policy Based Redirect



For N9K93128TX, N9K9396PX, and N9K9396TX switches, the service appliance must not be in the same leaf switch as either the source or destination endpoint group.

Basic Topology

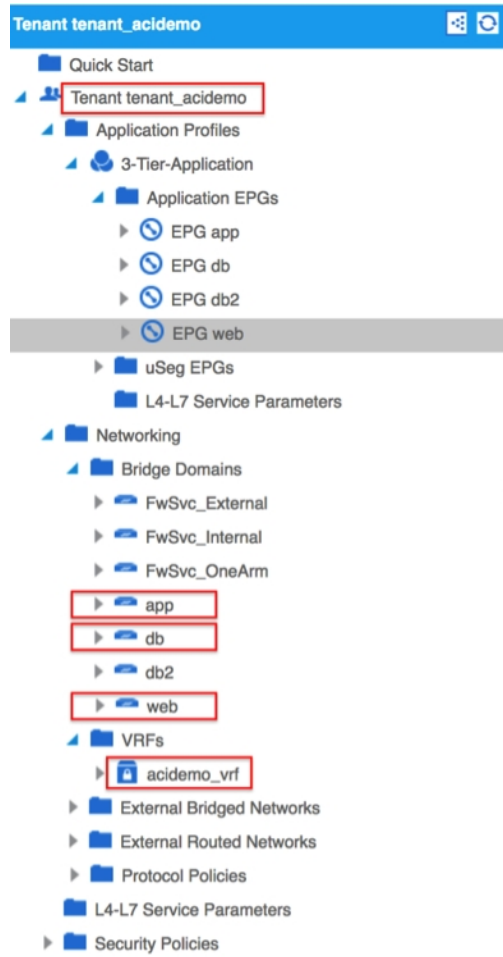


Work Flow:

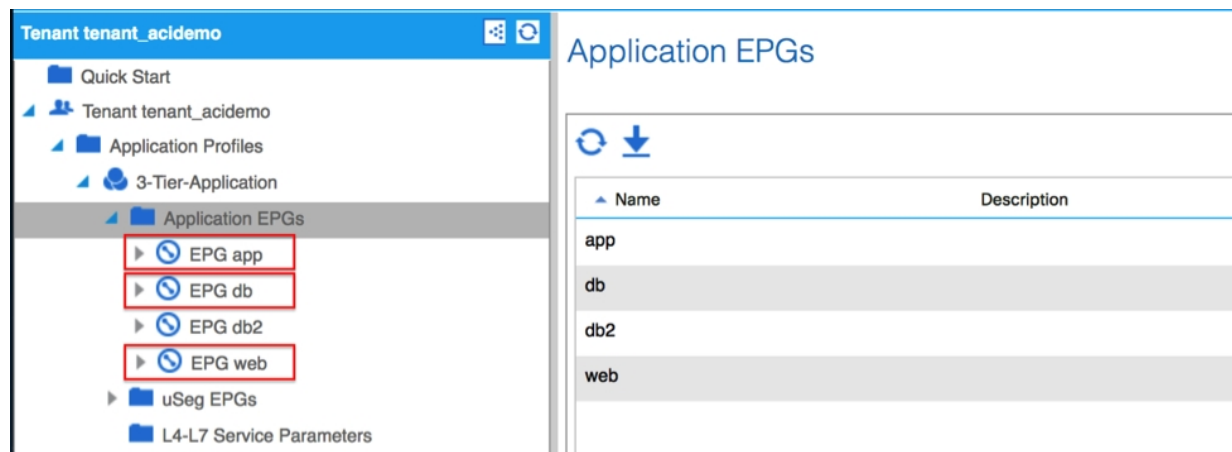
1. Create Tenant ("acidemo" in our example)
2. Create VRF ("acidemo_vrf" in our example)
3. Create 3 Bridge Domains ("web", "app", and "db" in our example)
4. Associate Bridge Domains to VRF
5. Create 3 EPGs ("web", "app", and "db" in our example)
6. Associate EPGs to Bridge Domains (EPG "web", "app", and "db" are mapped to Bridge Domain "web", "app", and "db" respectively in our example)
7. Create Dedicated Firewall Services Bridge Domain and Subnet on Cisco APIC
8. Create L4-L7 Policy Based Redirect on Cisco APIC
9. Create Go-To mode Device on Cisco APIC and define 2 logical interfaces
10. Create Functional Profile
11. Create Service Graph Template
12. Deploy Service Graph Template

Configuration

Create Tenant, VRF and 3 Bridge Domains on Cisco APIC



Create 3 EPGs



Associate EPG “web”, “app”, and “db” to Bridge Domain “web”, “app”, and “db” respectively

Web

The screenshot displays the FortiGate GUI configuration page for the EPG named 'web' under the tenant 'tenant_acidemo'. The left sidebar shows the configuration tree with 'EPG web' selected. The main panel shows the 'Properties' section for this EPG.

EPG - web

Properties

- Description: optional
- Tags: enter tags separated by comma
- Alias:
- uSeg EPG: false
- pcTag(sclass): 49159
- QoS class: Unspecified
- Custom QoS: select a value
- Intra EPG Isolation: **Enforced** Unenforced
- Preferred Group Member: **Exclude** Include
- Configuration Status: **applied**
- Configuration Issues:
- Label Match Criteria: AtleastOne
- Bridge Domain: tenant_acidemo/web
- Resolved Bridge Domain: tenant_acidemo/web
- Monitoring Policy: select a value

App

The screenshot displays the Cisco ACI GUI interface. On the left, a navigation pane shows the hierarchy: Tenant tenant_acidemo > Application Profiles > 3-Tier-Application > Application EPGs > EPG app (highlighted with a red box). Below this, a list of EPGs is shown, including EPG db, EPG db2, EPG web, uSeg EPGs, and L4-L7 Service Parameters. The main panel on the right is titled 'EPG - app' and shows the 'Properties' configuration page. The 'Description' field is set to 'optional'. The 'Tags' field is empty, with a hint 'enter tags separated by comma'. The 'Alias' field is empty. The 'uSeg EPG' is set to 'false'. The 'pcTag(sclass)' is '49157'. The 'QoS class' is 'Unspecified'. The 'Custom QoS' is 'select a value'. The 'Intra EPG Isolation' is set to 'Enforced'. The 'Preferred Group Member' is set to 'Exclude'. The 'Configuration Status' is 'applied'. The 'Configuration Issues' are empty. The 'Label Match Criteria' is 'AtleastOne'. The 'Bridge Domain' is 'tenant_acidemo/app' (highlighted with a red box). The 'Resolved Bridge Domain' is 'tenant_acidemo/app'. The 'Monitoring Policy' is 'select a value'. A green status bar at the top right of the main panel shows '100'.

DB

Tenant tenant_acidemo

EPG - db

Properties

Description: optional

Tags: enter tags separated by comma

Alias:

uSeg EPG: **false**

pcTag(sclass): **32775**

QoS class: **Unspecified**

Custom QoS: select a value

Intra EPG Isolation: **Enforced** **Unenforced**

Preferred Group Member: **Exclude** **Include**

Configuration Status: **applied**

Configuration Issues:

Label Match Criteria: **AtleastOne**

Bridge Domain: **tenant_acidemo/db**

Resolved Bridge Domain: **tenant_acidemo/db**

Monitoring Policy: select a value

Create Dedicated Firewall Services Bridge Domain and Subnet on Cisco APIC

Uncheck Endpoint Dataplane Learning and Create a Subnet. This Subnet IP will be used later in the default route on the Fortigate.

Tenant tenant_acidemo

Bridge Domain - FwSvc_OneArm

Properties

Name: **FwSvc_OneArm**

Description: optional

Type: **lc regular**

Alias:

Legacy Mode: **No**

VRF: **tenant_acidemo/acidemo_vrf**

Resolved VRF: **tenant_acidemo/acidemo_vrf**

L2 Unknown Unicast: **Flood** **Hardware Proxy**

L3 Unknown Multicast Flooding: **Flood** **Optimized Flood**

Multi Destination Flooding: **Flood in BD** **Drop** **Flood in Encapsulation**

PIM: ☐

IGMP Policy: select an option

ARP Flooding: ☒

Endpoint Dataplane Learning: ☐

End Point Retention Policy: select a value

This policy only applies to local L2, L3, and remote L3 entries

Create L4-L7 Policy Based Redirect on Cisco APIC

The IP Address will be the same IP assigned to the Fortigate internal interface later. The MAC Address is the same as the physical interface MAC on the Fortigate. This can be obtained with global Fortigate CLI command “diagnose hardware deviceinfo nic <port>”

The screenshot shows the Cisco APIC GUI with the left navigation pane expanded to 'L4-L7 Policy Based Redirect'. The main pane displays the configuration for 'FGT_OneArm'.

Properties

- Name: FGT_OneArm
- Description: optional
- Destinations:

IP	MAC
172.16.0.254	90:6C:AC:69:E8:CD

Create Device with Go-To mode with 2 logical interfaces on Cisco APIC (“internal” and “external”).

We will only utilize internal.

The screenshot shows the Cisco APIC GUI with the left navigation pane expanded to 'L4-L7 Devices'. The main pane displays the configuration for 'FGT1500D-1.3-OneArm'.

Managed: ☒ **Name:** FGT1500D-1.3-OneArm

Device Package: Fortinet-FGAPIC-1.3

Service Type: Firewall

Device Type: PHYSICAL

Physical Domain: FWDomain

Context Aware: Multiple

Function Type: GoThrough GoTo

Credentials

Username: root

Password: [REDACTED]

Confirm Password: [REDACTED]

Configuration State

Configuration Issues: stable

Devices

Name	Management Address	Management Port	Interfaces
Device1	10.100.21.39	443	port26 (Pod-1/Node-103/eth1/48)

Cluster

Management IP Address: 10.100.21.39

Management Port: 443

Device Manager: select a value

Cluster Interfaces:

Type	Name	Concrete Interfaces
consumer	external	Device1/port26
provider	internal	Device1/port26

Buttons: SHOW USAGE, SUBMIT, RESET

Create Functional Profile

Functional Profile defines the template for the Service(s) that is going to deploy such as L4-L7 Device Interface IP addresses, Rule ID, Object Addresses, Policy Rules, Source/Destination Ports...etc.

Create Function Profile

Name: L3_OneArm

Description: optional

Copy Existing Profile Parameters: ☒

Profile: Fortinet-FGAPIC-1.3/Basic-Firewall-Policy

Features and Parameters

In order to auto apply new values to the parameters of existing graph instance when users modify function profiles, the name of top folder must be ended with -Default.

Basic Parameters All Parameters

Folder/Param	Name	Value	Mandatory	Locked	Shared
Device Config	Device				
DeviceInterface	external			false	false
DeviceInterface	internal			false	false
Function Config	Function				
Network	Network			false	false

SUBMIT CANCEL

Functional Profile Objects Explanation:

Device Config

Contains External and Internal Interfaces that will be programmed onto Fortigate VDOM. This is the interfaces (typically external and internal) that will be associated to the VDOM. We will delete the external interface since it is not utilized.

Function Config

Function Config consist of:

- Network
 - This field is use for configure Static Routes for IPv4 and IPv6.
- Policy and Objects

This folder is the container for following list of folders:

- FWServiceFolder – Firewall Service Object container
- IPv4/IPv6 DoS Policy – Dos Policy configuration
- IPv4/IPv6 FirewallAddresses – Firewall Addresses Object container
- IPv4 Policy – Firewall Policy Rule container
- IPv4 FirewallAddresses Group – Group folder for “Dynamic EPG” feature
- ScheduleFolder – Schedule container

- VDOM-Folder
 - VDOM internal and external interfaces

For this use case, internal is going to be shared for all service graph deployments. The Device IP Address will need to match the Policy Based Routing destination. Change the VDOM interfaces both to internal.

Edit Function Profile

Click row to edit value

Features:

- DeviceNetwork
- FirewallObjects
- FirewallPolicyRule
- StaticRouter
- All

Folder/Param	Name	Value	Mandatory	Locked	Shared
Device Config	Device				
DeviceInterface	DeviceInterface	internal		false	false
AllowAccess	AllowAccess...			false	
Device IP Address...	IPAddress	172.16.0.254	false	false	
Device IP Netma...	IPNetmask	255.255.255.0	false	false	
Device IPv6 Add...	IPv6IPAddress	::	false	false	
Device IPv6 Net...	IPv6IPNetma...	0	false	false	
Interface Address...	mode	static	false	false	
Interface IPv6 Ad...	IPv6Mode	static	false	false	
Function Config	Function				
Network	Network			false	false
Policy and Objects	PolicyObjects			false	false
VDOM-Folder	vdom-folder			false	false
VDOM Interface ...	VDOM-exte...	internal	false	false	
VDOM Interface ...	VDOM-interna	internal	false	false	

SUBMIT **CANCEL**

A single default route is needed and should point to the Dedicated Firewall Services BD Subnet IP Address.

FEATURES AND PARAMETERS

Features:

- DeviceNetwork
- FirewallObjects
- FirewallPolicyRule
- StaticRouter
- All

Meta Folder/Param Key	Name	Value	Mandatory	Locked	Shared
Function Config	Function				
Network	Network			false	false
Static Routes	StaticRoutesF...			false	
IPv4 Static Route	IPv4StaticRoute			false	
IPv4 Static Route	IPv4StaticRou...			false	
Route Destination IP Address	DestinationIPA...	0.0.0.0	true	false	
Route Destination Netmask	DestinationNe...	0.0.0.0	true	false	
Device Interface	DeviceInterface	internal	true	false	
Administrative distance	Distance	10	true	false	
Gateway IP Address	GatewayIPAdd...	172.16.0.1	true	false	
Administrative priority	Priority	0	true	false	
Sequence Number of Route	SequenceNum...	10	true	false	

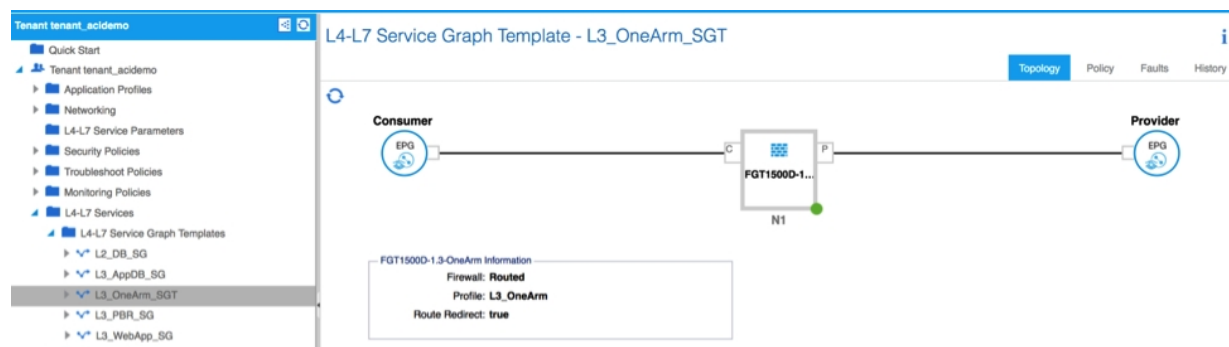
The Firewall Policies should utilize the same incoming and outgoing interfaces since this is a one-arm configuration.

FEATURES AND PARAMETERS

Features:	Basic Parameters					
	All Parameters					
DeviceNetwork	Meta Folder/Param Key	Name	Value	Mandatory	Locked	Shared
FirewallObjects	IPv4 FirewallAddresses	IPv4FWAddre...			false	
FirewallPolicyRule	IPv4 Policy	IPv4FWPolicy...			false	
StaticRouter	FirewallPolicyRuleID(Number Only - ...	10			false	
All	Action(accept/deny/ssl-vpn)	Action	accept	false	false	
	Destination Address or VIP	DestAddrVIP			false	
	Incoming interface(internal/extern...	InInterface	internal	false	false	
	LoggingOptions	Logging			false	
	Name	Name	internal	false	false	
	OrderNo	OrderNo	10	true	false	
	Outcoming interface(internal/exte...	OutInterface	internal	false	false	
	SecurityProfiles	SecurityProfiles			false	
	Source Address Folder	SrcAddrFolder			false	

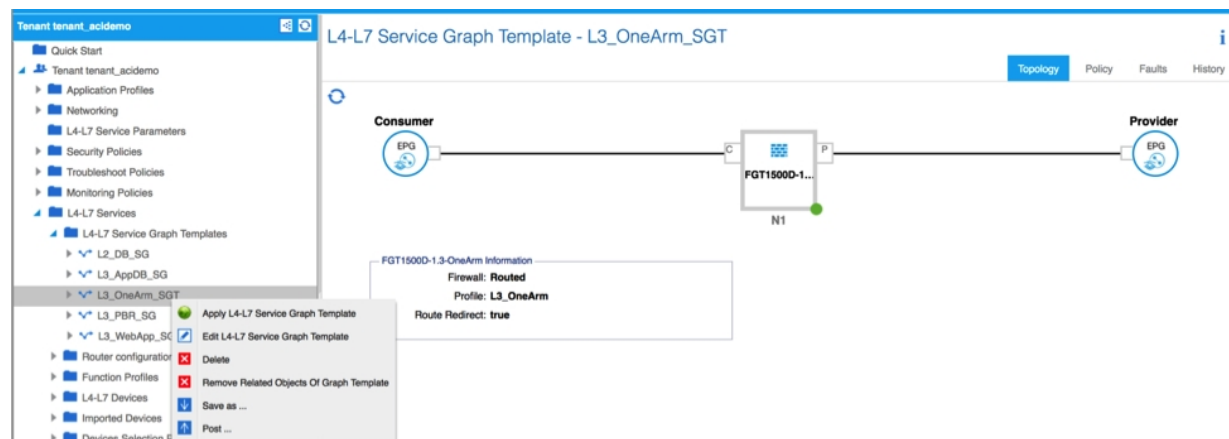
Create Service Graph1 for Web and App

Service Graph template is used to tightly coupled the Functional Profile or Firewall configuration and combine with the Firewall device we defined at earlier steps. (Please check “Route Redirect” option box to enable Policy Based Routing)



Deploy Service Graph1 Web to App

Once we combine the Firewall configuration and associated device together, we are ready to deploy Service Graph 1.



On next screen select the Consumer and provider EPGs (“Web” and “App”) and assign a contract name or select a pre-defined contract. For Policy Based Redirect, it is recommended to apply a filter and only redirect applicable traffic.

Apply L4-L7 Service Graph Template To EPGs

STEP 1 > Contract

1. Contract 2. Graph

Config A Contract Between EPGs

EPGs Information

Consumer EPG / External Network: **tenant_acidemo/3-Tier-Applicatio** Provider EPG / Internal Network: **tenant_acidemo/3-Tier-Applicatio**

Contract Information

Contract: ☒ Create A New Contract ☐ Choose An Existing Contract Subject

Contract Name: **acidemo-webtoapp**

No Filter (Allow All Traffic): ☐

Filter Entries:

Name	EtherType	ARP Flag	IP Protocol	Match Only Fragment	Stateful	Source Port / Range	Destination Port / Range	TCP Session Rules
IP	IP		unspecified	False	False			

Next screen select the logical interfaces (“app” and “web”) defined during the creation of Layer4-7 Device.

Tenant **tenant_acidemo**

Logical Interface Context - consumer

Properties

Connector Name: **consumer**

Cluster Interface: **internal**

Associated Network: **Bridge Domain** **L3 External Network**

Bridge Domain: **FwSvc_OneArm**

L4-L7 Policy Based Redirect: **tenant_acidemo/FGT_**

Permit Logging: ☐

Subnets:

IP/Mask	Scope
	No Select

Virtual IP Addresses:

IP Address	
	No Select

Due to an APIC GUI bug, it is necessary to select the incorrect BD now causing the SGT to fail to deploy. Select common/default, it will get remedied in the next steps.

Select the Device Selection Policy created by the previous step, consumer connector. Change to the correct BD, FwSvc_OneArm in our example. Make sure the cluster interface is set to internal.

The screenshot displays the FortiGate Connector GUI for a tenant named 'tenant_acidemo'. The left sidebar shows a tree view of configuration objects, with 'L4-L7 Services' expanded. Under 'L4-L7 Service Graph Templates', 'L3_OneArm_SGT' is selected. The main panel, titled 'Logical Interface Context - provider', shows the 'Properties' section. The 'Connector Name' is 'provider'. The 'Cluster Interface' is set to 'internal'. The 'Associated Network' is 'Bridge Domain', and the 'Bridge Domain' is 'FwSvc_OneArm'. The 'L4-L7 Policy Based Redirect' is set to 'tenant_acidemo/FGT_'. The 'Permit Logging' checkbox is unchecked. Below the 'Subnets' section, there is a table with columns 'IP/Mask' and 'Scope'. The 'Virtual IP Addresses' section is also visible, with a sub-section for 'IP Address'.

Now change the provider connector. Change the BD and cluster interface.

Verify Service Graphs Deployment

The screenshot displays the FortiGate GUI interface for verifying service graph deployment. The left pane shows the 'Tenant tenant_acidemo' hierarchy, with 'Deployed Graph Instances' selected. The right pane shows the 'Deployed Graph Instances' table.

Service Graph	Contract	Contained By	State
L3_OneArm_SGT	acidemo-webtoapp	Tenant tenant_acidemo	applied

Verify Device Deployment

Virtual Device - FGT1500D-1.3-OneArm-acidemo_vrf

Policy

100

Properties

Devices: **FGT1500D-1.3-OneArm**

Virtual Device ID: **5795**

VRF: **acidemo_vrf**

Operational State: **stable**

ACKed Transaction ID: **10002**

Current Transaction ID: **10002**

Cluster Interfaces:

Logical Interface	Encap
FGT1500D-1.3-OneArm_internal	vlan-972

The Virtual Device ID is the VDOM ID which has been deployed to the Fortigate. The VLAN indicated has been applied to the interface created on the Fortigate under this VDOM for the internal interface.

Verify Fortigate Deployment

Verify the Network interface has been configured correctly.

FortiGate 1500D FG1K5D3I16802243

5795

FortiView

Network

Interfaces

Packet Capture

WAN LLB

WAN Status Check

WAN LLB Rules

Static Routes

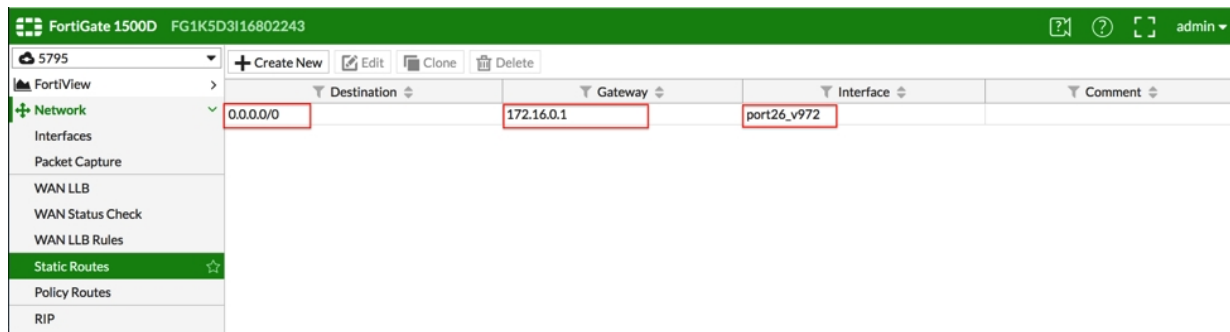
Policy Routes

Create New Edit Delete

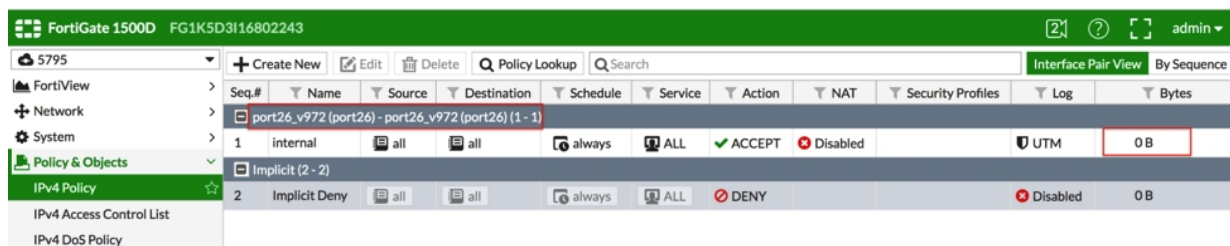
By Type By Role Alphabetically

Status	Name	Members	IP/Netmask	Type	Access	Virtual Domain	Ref.
Physical (2)	port26		0.0.0.0/0.0.0.0	Physical Interface		root	1
	port26_v972		172.16.0.254/24	VLAN	PING	5795	3

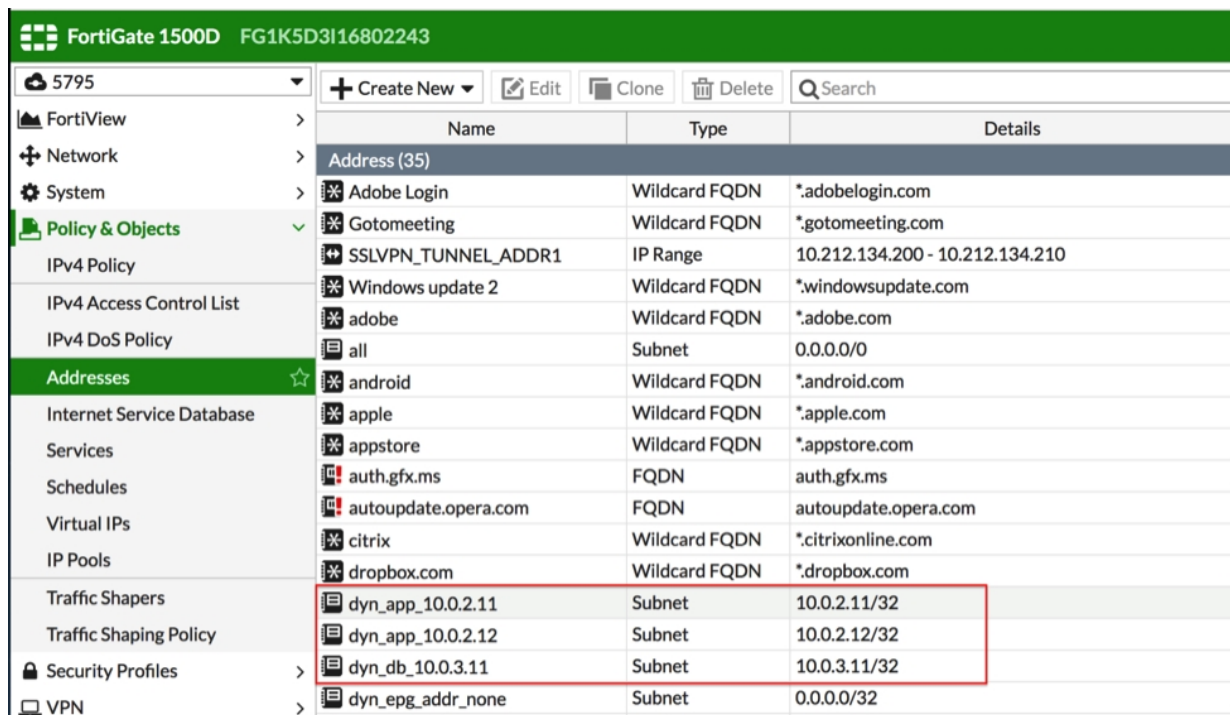
Verify the static route has been configured correctly.



Verify the Firewall Policy has been configured correctly. This policy shows traffic incoming and outgoing on same interface. No traffic has been seen yet matching this policy.



Verify the dynamic EPG address group has been updated.



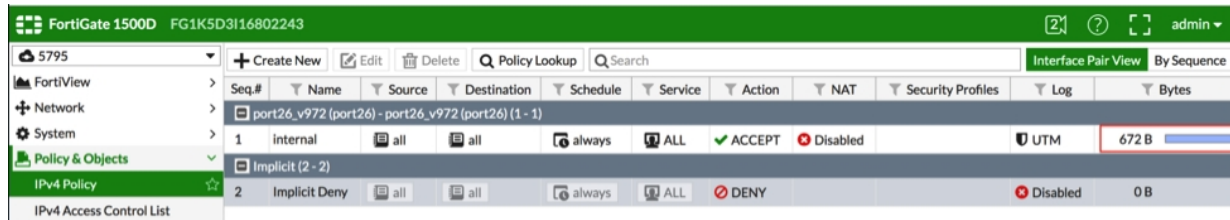
Generate some traffic such as ping to verify connectivity.

```

root@App01:~# ping 10.0.3.11
PING 10.0.3.11 (10.0.3.11) 56(84) bytes of data.
64 bytes from 10.0.3.11: icmp_req=1 ttl=59 time=1.68 ms
64 bytes from 10.0.3.11: icmp_req=2 ttl=59 time=0.623 ms
64 bytes from 10.0.3.11: icmp_req=3 ttl=59 time=0.666 ms
64 bytes from 10.0.3.11: icmp_req=4 ttl=59 time=0.677 ms
^C

```

Check to see if the counters have increased.



Seq.#	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
1	Internal	all	all	always	ALL	ACCEPT	Disabled	UTM		672 B
2	Implicit Deny	all	all	always	ALL	DENY		Disabled		0 B

APIC Infrastructure and FortiGate rollback

1. Upload and unload device package
2. Add and Delete device, FortiGate should clean-up previous configuration.
3. Dynamically modify and update policies
4. Detach and Attach service graphs
5. Delete tenants while service graphs in use.

Basic Troubleshooting

Verify Service Graph deployed

If Service Graph Deployed failed:

Navigate under **Tenant > Deployed Graph Instances** to check the state of the deployed graph.

If state is **failed apply**, then go down one level to the **Deployed Graph Instances** and navigate to the **Fault** tab to check the error log. Any error code in 1000 range are relating to FortiGate while others belong to APIC

Currently we only have the following error code:

Error Code	Definition
1010	Configuration Error in device configuration
1020	Configuration Error in function configuration
1030	Internal Error -3
1040	Internal Error -4
1050	Internal Error -5
1070	Feature not available

The screenshot shows the Cisco ACI configuration interface for Tenant Ten2. The left sidebar contains a tree view of configuration objects, including Application EPGs, Contracts, Static Bindings, Subnets, Domains, VM Attributes, Management IP Address Pools, L4-L7 Service Parameters, EPG Out, EPG Test, EPG Test3, EPG test2, L4-L7 Service Parameters, Networking, L4-L7 Service Parameters, Security Policies, Troubleshoot Policies, Monitoring Policies, L4-L7 Services, L4-L7 Service Graph Templates, DemoServiceGraph, Test2SG, Function Node - Firewall, Function Profiles, DemoFGroup, ProfileGroup, Test2, L4-L7 Devices, FGVM1000, Imported Devices, Devices Selection Policies, Deployed Graph Instances, L3contract-Test2SG-Ten2, and Deployed Devices.

The main panel displays the 'Deployed Graph Instances' table:

CONTRACT	STATE	SERVICE GRAPH	CONTAINED BY	FUNCTION NODES
L3contract	failed-to-apply	Test2SG	Tenant: Ten2	Firewall

The screenshot shows the Cisco ACI configuration interface for Tenant Ten2, specifically the 'L4-L7 Service Graph Instance - democontract-Test2SG-Ten2' page. The left sidebar contains a tree view of configuration objects, including Quick Start, Tenant Ten2, Application Profiles, Networking, L4-L7 Service Parameters, Security Policies, Troubleshoot Policies, Monitoring Policies, L4-L7 Services, L4-L7 Service Graph Templates, DemoServiceGraph, Test2SG, Function Profiles, DemoFGroup, ProfileGroup, L4-L7 Devices, FGVM1000, Imported Devices, Devices Selection Policies, Deployed Graph Instances, democontract-Test2SG-Ten2, Function Node - Firewall, Deployed Devices, FGVM1000-network1, IGP Device Configuration, OSPF Device Configuration, and democontract-Test2SG-Ten2.

The main panel displays the 'L4-L7 Service Graph Instance - democontract-Test2SG-Ten2' table with error details:

SEVERITY	ACKNOWLEDGED	CODE	CAUSE	CREATION TIME	LAST TRANSITION	AFFECTED OBJECT	LIFECYCLE	DESCRIPTION
Warning		P0758	graph-rendering-failed	2015-09-17T16:15:41.725-07:00	2015-09-17T16:18:50.373-07:00	uni/tn-Ten2/GraphInst-C[uni/tn-Ten2/democontract-Test2SG-Ten2]	Retaining	Service graph for tenant Ten2 could not be instantiated. Info: L4-L7 Devices FGVM1000
Warning		F1307	resolution-failed	2015-09-17T16:15:41.568-07:00	2015-09-17T16:16:44.214-07:00	uni/tn-Ten2/GraphInst-C[uni/tn-Ten2/democontract-Test2SG-Ten2]	Retaining	Failed to form relation to HG uni/tn-Ten2/Device-Profile-1000-Firewall/mcConn-external of class vnshConn
Warning		F1307	resolution-failed	2015-09-17T16:15:41.670-07:00	2015-09-17T16:16:44.222-07:00	uni/tn-Ten2/GraphInst-C[uni/tn-Ten2/democontract-Test2SG-Ten2]	Retaining	Failed to form relation to HG uni/tn-Ten2/Device-Profile-1000-Firewall/mcConn-internal of class vnshConn

Service deployed but parameters missing

If Service deployed but certain parameters not showing up on Fortigate, please follow the below steps:

1. Navigate to **Tenant > Provider EPG > L4-L7 Parameters**, ensure the missing parameters are listed. If not, double check the functional profile to confirm the configuration

Figure 1.

Your Cluster contains less than 3 In-Service Controllers. Please Backup the cluster and not utilize the fabric in its current state for production.

L4-L7 Service Parameters					
META FOLDER/PARAM KEY	CONTRACT NAME	SERVICE GRAPH NAME	SERVICE FUNCTION NAME	FOLDER/PARAM INSTANCE NAME	VALUE
FirewallPolicyRule	democontract	Test25G	Firewall	10	
FirewallPolicyRule	democontract	Test25G	Firewall	20	
FirewallService	democontract	Test25G	Firewall	ALL	
FirewallService	democontract	Test25G	Firewall	ALL_ICMP	
FirewallService	democontract	Test25G	Firewall	ALL_TCP	
FirewallService	democontract	Test25G	Firewall	ALL_UDP	
FirewallAddress	democontract	Test25G	Firewall	Adobe_Login	
DeviceRouter	democontract	Test25G	Firewall	DeviceRouter-Default1	
FirewallAddress	democontract	Test25G	Firewall	Gotomeeting	
FirewallService	democontract	Test25G	Firewall	HTTP	
FirewallService	democontract	Test25G	Firewall	HTTPS	
FirewallAddress	democontract	Test25G	Firewall	None	
FirewallAddress	democontract	Test25G	Firewall	SSLVPN_TUNNEL_ADDR1	
VDOM	democontract	Test25G	Firewall	VML2	
FirewallAddress	democontract	Test25G	Firewall	Windows_update_2	
FirewallAddress	democontract	Test25G	Firewall	adobe	
FirewallAddress	democontract	Test25G	Firewall	all	
ScheduleRecurring	democontract	Test25G	Firewall	always	
FirewallAddress	democontract	Test25G	Firewall	android	
FirewallAddress	democontract	Test25G	Firewall	apple	
FirewallAddress	democontract	Test25G	Firewall	appstore	
FirewallAddress	democontract	Test25G	Firewall	auth.gfx.ms	
FirewallAddress	democontract	Test25G	Firewall	autoupdate.opera.com	
FirewallAddress	democontract	Test25G	Firewall	citrix	
FirewallAddress	democontract	Test25G	Firewall	dropbox.com	

- If yes, login on to Cisco APIC controller to examine the debug log. The debug log is located at `/data/devicescript/Fortinet.FGAPIC.1.3/logs` and the log file name is `debug.log`. Examine the log file and grab fields with "[10.160.11.103, <xxxx>]:" formats and scan through the logs associated to the parameters in question.
- If all failed, please forward the entire captured log to Fortinet Technical Assistance Center for further troubleshooting.



FORTINET®

High Performance Network Security



Copyright© 2017 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.